Points à examiner à l'approche des négociations de Phase II de la ZLECAf : enjeux de la politique commerciale numérique dans quatre pays d'Afrique subsaharienne

Rapport sur la politique

DOI: https://doi.org/10.35489/BSG-DP-WP_2022/01

Préparé par
Rutendo Tavengerwei, Valary Mumbo
et Beatriz Kira

United Nations
Economic Commission for Africa

Digital Pathways at Oxford

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD

Beatriz Kira *et* Rutendo Tavengerwei, *Digital Pathways, Blavatnik School of Government, Université d'Oxford,*
et Valary Mumbo, *maîtrise en politique publique, Blavatnik School of Government, Université d'Oxford*

Document 16
Janvier 2022

Digital Pathways at Oxford est un programme de recherche basé à la Blavatnik School of Government de l'Université d'Oxford. Il produit des recherches de pointe dans de multiples secteurs ; politique publique, droit, économie, sciences informatiques et sciences politiques, afin de contribuer à des prises de décision éclairées quant à la gouvernance des technologies numériques, en ciblant plus spécifiquement les pays à faibles et moyens revenus.

Ce document fait partie d'un ensemble de rapports sur les politiques et les réglementations en matière de technologie, regroupant des preuves, des idées et de nouvelles recherches sur les forces et les faiblesses de pratiques émergentes dans des pays en développement. Les opinions et les positions exprimées dans ce document sont celles de l'auteur et ne représentent pas l'Université d'Oxford.

Citation :
Tavengerwei, R., Mumbo, V. et Kira, B. (2022). *Points à examiner à l'approche des négociations de Phase II de la ZLECAf : enjeux de la politique commerciale numérique dans quatre pays d'Afrique subsaharienne.* Série de documents de Digital Pathways at Oxford, n°16. Oxford, Royaume-Uni

https://www.bsg.ox.ac.uk/research/research-programmes/digital-pathways

United Nations
Economic Commission for Africa

Digital Pathways at Oxford

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

@DigiPathOxf
Image de couverture : © Shutterstock

United Nations
Economic Commission for Africa

Digital
Pathways
at Oxford

BLAVATNIK
SCHOOL OF
GOVERNMENT

UNIVERSITY OF
OXFORD

Remerciements

Les auteurs souhaitent remercier les personnes interrogées pour leur contribution précieuse à cette étude. Pour la perspicacité de nos échanges et leurs commentaires pertinents quant aux précédentes versions de ce rapport, nous remercions Emily Jones, Elizabeth Stuart, Danilo Barbosa Garrido Alves, Ify Ogo, David Luke, Jamie McLeod, Vahini Naidu, Vitor Ido, Melissa Omino, Dennis Muhambe, Mohamed Diop, Laura Naliaka, Faizel Ismail, Penny Parenzee, Karishma Banga, Franziska Sucker, Aileen Kwa, Quan Zhao et Gervais Mendy. Pour son appui au financement de la recherche ayant donné lieu à ce rapport, nous remercions l'Omidyar Network. Pour ses commentaires initiaux et son soutien dans la diffusion des résultats, nous remercions la Commission économique des Nations unies pour l'Afrique. Pour leur soutien lors de la révision et de la mise en page de ce rapport, nous remercions Kirsten Hunter, Beth Keehn et Nic Farrell.

Table des matières

Tableaux

Figures

Abréviations

ZLECAf - Zone de libre-échange continentale africaine
ARIPO - African Regional Intellectual Property Organization CAE - Communauté d'Afrique de l'Est
CEDEAO - Communauté économique des États de l'Afrique de l'Ouest
ECTA - Loi sur les communications et transactions électroniques d'Afrique du Sud ALE - Accord de libre-échange
TIC - Technologies de l'information et de la communication
RGPD - Règlement général sur la protection des données de l'Union européenne NITDA - Agence nationale de développement des technologies de l'information NDPR - Règlement nigérian sur la protection des données
OAPI - Organisation africaine de la propriété intellectuelle
OSS - logiciel libre
CDAA - Communauté de développement de l'Afrique australe
ADPIC - Accord de l'OMC sur les aspects des droits de propriété intellectuelle qui touchent au commerce CNUDCI - Commission des Nations unies pour le droit commercial international
CNUCED - Conférence des Nations unies sur le commerce et le développement ACEUM - Accord Canada–États-Unis–Mexique
OMC - Organisation mondiale du commerce

1. Synthèse

La conjoncture, notamment la pandémie de COVID-19, a accéléré la transition vers des opérations en ligne, soulignant un fait indéniable : le monde poursuit sa conversion numérique. Plus que jamais, les décideurs doivent donc légiférer de manière à tirer parti des avantages du commerce numérique tout en évitant les risques associés. Toutefois, du fait de l'absence de coordination mondiale du commerce numérique, les pays adoptant diverses stratégies vis-à-vis des enjeux des politiques, une divergence perdure au niveau des réglementations nationales et limite les avantages offerts par le commerce électronique aux pays. Compte tenu de ces disparités et en prévision des négociations de Phase II de la Zone de libre-échange continentale africaine (ZLECAf), des pays africains ont réfléchi à la meilleure façon d'harmoniser les réglementations dans le secteur du commerce numérique. Pour procéder efficacement, les membres de la ZLECAf doivent identifier les zones de divergence entre leurs systèmes de réglementation nationaux. Ainsi, les membres de la ZLECAf pourront déterminer où une harmonisation est possible et quels sont les éléments nécessaires à cette fin.

Ce rapport analyse les réglementations et les politiques nationales de quatre pays : l'Afrique du Sud, le Nigeria, le Kenya et le Sénégal. Il compare leurs stratégies réglementaires quant à cinq enjeux de politiques : i) la régulation des transactions en ligne, ii) les flux de données transfrontaliers, la localisation de données et la protection des données personnelles, iii) l'accès au code source et le transfert de technologie, iv) la responsabilité des intermédiaires et v) les droits de douane sur les transmissions électroniques. L'étude souligne les divergences actuelles des stratégies adoptées, pointant la nécessité pour les quatre pays (et les membres de la ZLECAf engénéral) d'examiner soigneusement les répercussions de ces divergences et de déterminer où il est possible et bénéfique d'harmoniser ces stratégies. L'objectif est d'encourager les États membres de la ZLECAf à s'approprier ces enjeux et à réfléchir aux réformes requises.

Comme l'indique le Tableau 1 ci-dessous, l'étude montre que les quatre pays divergent sur la plupart des cinq enjeux de politiques. Il existe des différences dans la manière dont ils réglementent les transactions en ligne, c'est-à-dire les signatures électroniques et la protection du consommateur en ligne. Parmi ces quatre pays, le Nigeria est le seul à reconnaître tous les types de signatures électroniques comme étant juridiquement équivalents. Le Kenya et le Sénégal ne reconnaissent que certaines signatures électroniques, émises ou validées par une institution reconnue, tandis que l'Afrique du Sud adopte une stratégie mixte, reconnaissant la validité juridique de toutes les signatures électroniques mais accordant une valeur probante supérieure à certains types de signatures électroniques. Seuls l'Afrique du Sud et le Sénégal disposent de réglementations spécifiques quant à la protection du consommateur en ligne. Le Nigeria et le Kenya n'ont pas de règles claires.

Pour les flux de données transfrontaliers, la localisation de données et la protection des données personnelles, l'étude montre que les quatre pays cibles disposent de régulations composées d'éléments empruntés au Règlement général sur la protection des données (RGPD) de l'Union européenne (UE). Cela concerne plus spécifiquement la demande de consentement du sujet des données et l'exigence d'adéquation. Fait intéressant, l'étude indique également que l'Afrique du Sud, le Kenya et le Nigeria adoptent aussi des mesures de localisation des données, même s'ils

appliquent divers degrés de rigueur. Les lois de l'Afrique du Sud sur la localisation des données régissent principalement les données considérées sensibles (qui doivent être traitées au sein des frontières sud-africaines), tandis que le Nigeria stipule que les données doivent être traitées et stockées localement via des serveurs locaux. Les mesures de localisation des données imposées par le Kenya concernent essentiellement la confidentialité des données, considérée comme une priorité. Des quatre pays cibles, le Sénégal est le seul à ne pas imposer de lois sur la localisation des données.

Bien que les quatre pays semblent privilégier la divulgation obligatoire du code source, l'étude démontre que leurs réglementations n'en sont pas aux mêmes stades. À l'heure actuelle, seul le Nigeria exige expressément que les entreprises multinationales divulguent le code source et les algorithmes de leurs logiciels avant de les déployer dans ce pays. Cette mesure s'applique par souci de sécurité. L'Afrique du Sud ne demande la divulgation obligatoire du code source que lorsque le logiciel doit être utilisé par le gouvernement, tandis que le Kenya promeut uniquement l'utilisation de logiciels libres pour les services publics. Le Sénégal est le seul pays sans régulations spécifiques quant à la divulgation du code source, bien qu'il ait exprimé un intérêt à l'égard d'une divulgation obligatoire du code source pour les services publics.

Comme l'indique le Tableau 1, il existe également des disparités dans la façon dont les quatre pays cibles régulent la responsabilité des intermédiaires. Si l'Afrique du Sud et le Sénégal dégagent tous deux les intermédiaires de toute responsabilité lorsque ceux-ci n'ont pas connaissance de la nature du contenu transmis ou stocké sur leur plateformes, le Nigeria ne pénalise les intermédiaires que lorsqu'ils ont connaissance du contenu illégal présent sur leurs plateformes mais ne le retirent pas. Le Kenya suit une approche plus stricte, criminalisant toute publication de fausses données ou de fake news, une distribution illicite, etc.

Même si l'étude montre que les quatre pays partagent une position commune à l'égard des droits de douane sur les transmissions électroniques, il est intéressant de noter qu'aucun d'eux ne dispose pour l'heure de réglementations ou de politiques nationales dans ce domaine.

Le rapport conclut en soulignant que, les négociations de Phase II de la ZLECAf visant une harmonisation et l'amélioration du commerce intra-africain et du commerce international, les membres de la ZLECAf doivent réfléchir à leur politiques et réglementations nationales pour déterminer quelles sont les harmonisations requises et si la ZLECAf est la bonne plateforme pour y parvenir efficacement.

Tableau 1 : Synthèse des stratégies vis-à-vis des divers enjeux des politiques

Pays		Afrique du Sud	Nigeria	Kenya	Sénégal
Enjeux des	a. Réglementation des transactions en ligne (signatures électroniques + protection du consommateur en ligne)	• N'établit aucune discrimination entre les divers types de signatures électroniques mais accorde davantage de valeur probante à certaines caractéristiques de signatures électroniques • Prévoit une réglementation spécifique sur la divulgation d'informations par un fournisseur, les spams, etc.	• Reconnaît tous les types de signatures électroniques comme juridiquement équivalents • Ne dispose pas encore de lois claires sur la protection du consommateur en ligne	• Reconnaît uniquement la validité des signatures électroniques avancées émises par un prestataire de services de certification • Ne dispose pas encore d'une législation spécifique sur la protection du consommateur en ligne	• Reconnaît uniquement la validité des signatures électroniques confirmées par des entreprises choisies • Prévoit une réglementation spécifique sur la divulgation d'informations, les modes de paiement, les conditions de garantie, etc.
	b. Flux de données transfrontaliers	• Associe des éléments du RGPD de l'UE, comme le consentement du détenteur des données, et des éléments de localisation des données, par exemple l'obligation de traiter et de stocker toutes les données jugées sensibles au sein des frontières de l'Afrique du Sud.	• Associe des réglementations de protection des données similaires au RGPD de l'UE pour le consentement et le respect de règles strictes de localisation des données, par exemple l'obligation pour les entreprises de télécommunication d'héberger toutes les données d'abonnés et de consommateurs au Nigeria. Les entreprises d'informations de données doivent également héberger les données nationales au Nigeria.	• Applique des lois de protection des données similaires à celles du RGPD de l'UE, par exemple le consentement du détenteur des données et l'obligation de conformité, associées à des éléments de localisation des données comme l'obligation de traiter les données destinées à un service public via des serveurs locaux.	• Suit étroitement la directive abrogée 95/46/CE de l'UE sur la protection des données, par exemple l'obligation d'obtenir le consentement du sujet des données et l'existence de motifs légitimes, explicites et spécifiques pour justifier un transfert.

	c. Accès au code source et transfert de technologie	• Requiert la divulgation obligatoire du code source des logiciels utilisés par le gouvernement.	• Requiert la divulgation obligatoire du code source et des algorithmes des entreprises multinationales avant le déploiement de logiciels au Nigeria.	• Encourage l'utilisation de logiciels libres dans l'administration publique.	• Ne dispose pas de réglementation spécifique sur le partage de code source.
	d. Responsabilité des intermédiaires	• Dégage uniquement les intermédiaires de toute responsabilité lorsque ceux-ci n'ont pas connaissance de la nature illicite du contenu qu'ils ont transmis, mis en cache, stocké ou hébergé.	• Exige que les intermédiaires retirent le contenu lorsqu'ils ont eu connaissance de son illégalité.	• Criminalise la publication de fausses données ou de fake news, la distribution illicite de messages obscènes ou intimes, la fraude informatique, etc.	• Dégage les intermédiaires de toute responsabilité lorsque ceux-ci n'ont pas connaissance de la nature du contenu qu'ils ont stocké.
	e. Droits de douane sur toutes les transmissions électroniques	Aucun des quatre pays n'a encore de législation sur les droits de douane appliqués aux transmissions électroniques. La position des quatre pays à l'Organisation mondiale du commerce est que l'interdiction des droits de douane sur les transmissions électroniques nuirait aux pays en développement.			

2. Introduction

Avec les progrès de la technologie, le commerce numérique est en hausse partout dans le monde, mû par l'expansion de l'accès à la technologie et à Internet, ainsi que par la volonté des pays de maximiser les opportunités et les retombées économiques offertes par le commerce numérique. Plus spécifiquement, les modèles économiques continuant de s'adapter aux développements technologiques, les individus et les entreprises de diverses juridictions peuvent plus facilement échanger et se coordonner rapidement au sein de chaînes de valeur mondiales, avec des coûts opérationnels moindres que ceux du commerce traditionnel. Par conséquent, les entreprises ont étendu leur portée et peuvent désormais vendre leurs produits sur davantage de marchés à l'échelle mondiale. Si le commerce numérique connaissait déjà une forte croissance avant la pandémie de COVID-19, l'obligation de s'appuyer principalement sur des transactions à distance a accéléré ce processus.

Bien que les progrès technologiques et la transition rapide vers des activités en ligne marquent un changement positif, ils suscitent plusieurs problèmes. Une fracture numérique considérable existe entre les pays développés et ceux en développement. La plupart des pays développés peuvent exploiter des opportunités d'investissement précoce dans la technologie, obtenant ainsi de plus vastes parts de marché et un avantage concurrentiel[4]. Cela leur permet de diriger le développement des stratégies réglementaires grâce auxquelles leurs économies bénéficient du commerce numérique. Les pays en développement prennent donc du retard et se voient parfois forcés d'adopter des stratégies fixes. Cependant, la stratégie industrielle numérique de la Chine ayant entraîné une augmentation de la part de son produit intérieur brut (PIB) de 26,1 % en 2014 à 34,8 % en 2018[5], d'autres pays en développement ont été incités à développer des stratégies réglementaires similaires pour rattraper leur retard dans l'industrialisation et devenir compétitifs sur le marché mondial.

Compte tenu des risques associés au commerce numérique, les pays du monde entier ont commencé à traiter un large éventail de questions transversales et à établir des réglementations pour profiter des bénéfices économiques. Ces questions incluent les règles liées à des thèmes tels que : le commerce dématérialisé, la fiscalité du numérique, les pratiques réglementaires favorisant la compétitivité numérique, la protection du consommateur en ligne, les transferts de données transfrontaliers, la responsabilité des intermédiaires, la divulgation du code source, les droits de douane sur les transmissions électroniques, etc. En dépit d'efforts de l'Organisation mondiale du commerce (OMC) sous l'Initiative de déclaration conjointe (IDC) et d'autres instances, comme l'Organisation de coopération et de développement économiques (OCDE), pour créer une stratégie réglementaire multilatérale vis-à-vis de certaines questions, l'absence de consensus sur la manière de légiférer a mené l'élaboration de règles mondiales dans une impasse. Par conséquent, pour fixer des normes relatives au commerce numérique qui incluent une dimension internationale et réduisent le risque de conflit commercial, les pays ont proactivement négocié et approuvé des règles via des accords commerciaux bilatéraux et multilatéraux, par exemple l'Accord de partenariat transpacifique global et progressiste (PTPGP), l'Accord de partenariat sur l'économie numérique (APEN), l'Accord Canada–États-Unis–Mexique (ACEUM), etc. Les pays s'assurent ainsi d'appliquer les deux aspects majeurs du commerce international : la clause de la nation la plus favorisée et le principe du traitement national. En plus de réglementer des accords commerciaux, de nombreux pays tels que le Royaume-Uni, les

États-Unis, la Chine et l'Australie ont été au premier plan lors du développement de leurs propres stratégies réglementaires nationales, certaines de ces stratégies apparaissant ensuite dans des accords commerciaux connexes. En a émergé un écosystème de règles fragmenté.

Les pays africains, en revanche, ont peu participé au processus décisionnel concernant le commerce numérique, aussi bien au niveau multilatéral que plurilatéral ou bilatéral. Plus précisément, au moment de la rédaction du présent rapport, seuls quatre pays africains participaient activement à des discussions de l'IDC de l'OMC[6] et seulement 25 faisaient partie du Cadre inclusif de l'OCDE[7]. De plus, à l'exception d'initiatives régionales, les pays africains ont peu participé aux accords commerciaux bilatéraux ou plurilatéraux ciblant le commerce. C'est pourquoi les pays africains commencent à subir une pression à l'égard des négociations bilatérales, par exemple les négociations de l'accord commercial entre les États-Unis et le Kenya.

Compte tenu des gains potentiels du commerce numérique et des avancées d'autres pays (en particulier les pays développés) dans la réglementation favorable pour eux de questions connexes, la région africaine doit soigneusement considérer comment développer et implémenter au mieux des réglementations harmonisées et adaptées à la région. Notamment, la Zone de libre-échange continentale africaine (ZLECAf), signée par 54 des 55 États membres de l'Union africaine et (au moment de la rédaction), ratifiée par 41[8], pourrait être la plateforme qui permettra de concrétiser ces objectifs pour la région. Il est donc important, avant les négociations sur le protocole de Phase II de la ZLECAf, que ses membres examinent toutes les questions liées au commerce numérique dans le contexte de leurs priorités nationales et régionales, sociales et économiques, en tenant compte des répercussions des diverses stratégies internationales, avant de les adopter définitivement ou de les rejeter. Cela permettra en outre aux membres de la ZLECAf d'identifier des opportunités de création de règles sur mesure favorables au commerce intrarégional sur le continent et avec le reste du monde. C'est un point important, car les dispositions négociées lors des accords commerciaux, qu'ils soient bilatéraux, régionaux ou plurilatéraux, peuvent entraver ou soutenir la prise de décision nationale ou régionale (ou en fin de compte, mondiale) et les efforts de réglementation visant à tirer parti des bénéfices de la numérisation.

Sur le plan de la méthodologie générale, ce rapport effectue une analyse comparative des différentes stratégies réglementaires et de politiques adoptées par les quatre pays cibles (l'Afrique du Sud, le Kenya, le Nigeria et le Sénégal) sur cinq enjeux de politiques spécifiques. Ces pays ont été choisis parce qu'ils constituent des économies majeures de la région et prennent en général une part active aux négociations commerciales, disposent de secteurs technologiques porteurs et participent proactivement à la réglementation du commerce numérique. Les principaux enjeux de politiques analysés ont été sélectionnés en fonction des tendances émergentes de questions clés négociées ou étant des dispositions d'accords commerciaux internationaux[9], et pouvant donc faire partie des négociations de Phase II de la ZLECAf. Selon une étude de Burri et Polanco, ces questions incluent : la réglementation des transactions en ligne, les flux de données transfrontaliers, l'accès au code source et le transfert de technologie, la responsabilité intermédiaire et les droits de douane sur les transmissions électroniques[10].

En comparant systématiquement les stratégies réglementaires des quatre pays cibles, ce rapport identifie les divergences réglementaires existantes et offre aux décideurs, ceux des quatre pays et d'autres membres de la ZLECAf présentant des contextes et des intérêts

économiques similaires, un éclairage sur les diverses stratégies adoptées. Avec cet éclairage sur les questions que la ZLECAf cherche à harmoniser, les décideurs peuvent déterminer s'ils souhaitent effectivement harmoniser les stratégies et, si oui, lesquelles sont les plus efficaces.

3. Détails des enjeux des politiques

Cette partie du rapport traite chacun des cinq enjeux majeurs des politiques. Le rapport détaille comment chaque enjeu est régulé à l'échelle internationale et souligne les conflits potentiels de ces stratégies réglementaires pour la région africaine en cas d'adoption par la ZLECAf. Pour chaque enjeu de politique, le rapport effectue une analyse comparative des stratégies réglementaires adoptées par chacun des quatre pays cibles et met en évidence les zones de divergence.

3.1 Réglementation des transactions en ligne

L'augmentation mondiale des achats en ligne accroît la pertinence des solutions numériques, par exemple les signatures électroniques facilitant les transactions en ligne, et renforce la nécessité de protéger le consommateur en ligne. Il est donc de plus en plus urgent que les pays s'assurent de réglementer les transactions en ligne de manière à favoriser la confiance, aussi bien des consommateurs que des prestataires de services.

3.1.1 Signatures électroniques

Les signatures électroniques constituent une composante essentielle du commerce numérique, car elles facilitent la conclusion de contrats commerciaux à distance entre les consommateurs et les prestataires de service. Les signatures électroniques ont également joué un rôle déterminant pour permettre les transactions transfrontalières entre entreprises lorsqu'un contrat avec des conditions spécifiques est nécessaire pour maintenir une relation d'affaires durable. Toutefois, malgré le rôle des signatures électroniques dans le commerce transfrontalier, les pays n'en sont pas aux mêmes stades de réglementation et adoptent différentes positions à l'égard de la neutralité technologique, ainsi que de la légitimité et du traitement des signatures électroniques. Ceci signifie que même si les signatures électroniques sont acceptées dans plusieurs pays, le format des signatures électroniques reconnues comme juridiquement valables et équivalentes aux signatures manuscrites suscite toujours le désaccord.

Au niveau international, il n'existe pas encore d'instrument multilatéral contraignant régissant les signatures électroniques. Bien que plusieurs pays utilisent la Convention des Nations unies (ONU) sur l'utilisation de communications électroniques comme référence pour élaborer des lois promouvant la neutralité technologique et l'équivalence fonctionnelle entre les signatures électroniques et manuscrites, les gouvernements sont majoritairement divisés entre trois principales approches divergeant toutes au niveau du traitement juridique des signatures électroniques.

Figure 1 : Stratégies vis-à-vis de la réglementation des signatures électroniques

Stratégie minimaliste	Stratégie prescriptive	Stratégie hybride
Les pays acceptent toutes les formes de signatures électroniques ou numériques, par exemple les États-Unis et l'Australie	Les pays exigent que les parties d'une transaction utilisent une méthode ou une technologie spécifique autorisée par le gouvernement pour que la signature soit valide, par exemple l'Indonésie	Les pays acceptent toutes les formes de signatures électroniques ou numériques mais accordent une valeur probante supérieure à certains types, par exemple l'Afrique du Sud

Comme l'indique la figure 1, les stratégies réglementaires des signatures électroniques sont : minimaliste, prescriptive et hybride[14]. La stratégie minimaliste est principalement adoptée par des pays disposant d'un système de droit commun classique, par exemple les États-Unis et l'Australie. Avec cette stratégie, les pays encouragent la neutralité technologique, acceptant toutes les formes de signatures électroniques ou manuscrites[15] et laissant la décision de la forme choisie aux parties de la transaction[16]. Cette approche vise à offrir davantage de flexibilité et d'adaptabilité aux utilisateurs et est donc plus favorable aux consommateurs[17]. De plus, la flexibilité de la stratégie minimaliste est jugée favorable car elle permet au marché d'orienter le cap des signatures électroniques, sans étouffer l'innovation en les régissant excessivement[18].

Néanmoins, du fait du degré d'incertitude existant en ligne, la stratégie prescriptive est considérée comme un moyen d'assurer la fiabilité et la sécurité, et donc la confiance pour les utilisateurs en ligne[19]. Les pays ayant adopté la stratégie prescriptive, principalement des pays de droit civil, exigent que les parties d'une transaction se servent d'une méthode ou d'une technologie spécifique autorisée par le gouvernement[20]. Par exemple, pour qu'une signature électronique soit reconnue en Indonésie, elle doit avoir été créée via un fournisseur de certificats numériques homologué auprès du ministère de la Communication et de la Technologie, à l'aide de serveurs situés dans le pays. Cette stratégie a l'avantage de fournir une sécurité maximale aux utilisateurs.

La stratégie hybride (comme son nom l'indique), associe quant à elle des caractéristiques des stratégies minimaliste et prescriptive. Les pays qui adoptent la stratégie hybride, par exemple l'Afrique du Sud, le Brésil, la Chine et l'UE, donnent un statut légal à toutes les méthodes de signatures électroniques, bien qu'ils accordent une plus grande valeur probante à des méthodes pourvues de certaines caractéristiques, telles que les signatures numériques[22]. La stratégie hybride offre la flexibilité de la stratégie minimaliste et permet une neutralité technologique tout en bénéficiant de la sécurité juridique de la stratégie prescriptive.

Stratégies régionales vis-à-vis des signatures électroniques

Selon l'inventaire mondial de la cyberlégislation de la Conférence des Nations unies sur le commerce et le développement (CNUCED), seuls 33 pays de la région africaine disposent d'une législation sur les transactions électroniques, six ont des versions préliminaires et six autres n'ont aucune forme de législation[24]. Comme mentionné ci-dessous, les lois nationales des 33 pays enregistrés incluent un mélange des trois stratégies présentées dans la figure 1. Plus précisément, il existe une divergence entre les quatre pays ciblés par cette étude, allant d'une stratégie strictement minimaliste à hybride.

C'est un indicateur des différents intérêts des pays et une illustration de la difficulté à atteindre une éventuelle harmonisation des lois dans le cadre de la ZLECAf. Par ailleurs, la diversité des règles nationales et régionales sur les signatures électroniques et l'authentification complique le respect de la conformité pour les entreprises désireuses d'opérer dans plusieurs pays. Ceci rend plus difficiles les activités numériques transfrontalières et augmente le coût d'une présence sur plusieurs marchés. De plus, si des consommateurs d'autres juridictions de la ZLECAf souhaitent effectuer des transactions en ligne, ce manque de clarté à l'égard des normes juridiques pertinentes risque de fragiliser leur confiance vis-à-vis du commerce électronique[25]. Il est donc nécessaire pour les pays, avant les négociations de Phase II de la ZLECAf, de tenir compte des divergences présentées ci-après, ainsi que des coûts associés. Ainsi, les membres de la ZLECAf pourront envisager si, et comment, ils peuvent harmoniser ou coordonner les réglementations régionales. Ce sont des considérations essentielles si les décideurs veulent créer des solutions sur mesure, pratiques et réalisables afin de s'assurer d'éviter tout coût inutile pour les entreprises, en particulier les microentreprises et les petites et moyennes entreprises (PME).

Afrique du Sud

L'Afrique du Sud a toujours adopté une stratégie hybride à l'égard des signatures électroniques. Elle l'applique en vertu de la Loi sur les communications et transactions électroniques de 2002 (ECTA)[26], ce qui est compatible avec le principe de neutralité technologie de la loi type sur les signatures électroniques de la Commission des Nations unies pour le droit commercial international (CNUDCI). Si avec sa stratégie hybride l'Afrique du Sud n'établit aucune discrimination entre les divers types de signatures électroniques, les reconnaissant comme juridiquement équivalents[27], elle accorde davantage de valeur probante à certaines caractéristiques de signatures électroniques. Plus précisément, tous les produits à signature électronique des fournisseurs doivent être reconnus par le directeur général du ministère des Communications[28].

Nigeria

Le Nigeria, à l'inverse de l'Afrique du Sud, du Kenya et du Sénégal, applique une stratégie minimaliste pour réglementer les signatures électroniques. Conformément à ses engagements en vertu de la loi de 2015 sur les transactions électroniques de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), le Nigeria considère généralement les signatures électroniques comme fiables et contraignantes, sauf preuve du contraire[29]. D'après la loi sur la preuve de 2011 du Nigeria, une signature électronique peut être prouvée de quelque manière que ce soit. Ceci peut inclure des procédures préalables à une transaction et exigeant qu'un

individu prouve ou effectue des procédures de sécurité pour confirmer l'identité de son document électronique[30]. Il incombe donc à l'individu affirmant la validité de prouver l'authenticité de la signature électronique. L'approche minimaliste du pays est cohérente avec la loi type régionale stipulée par l'Acte additionnel portant transactions électroniques de 2010 de la CEDEAO.

Kenya

Le Kenya adopte une stratégie prescriptive pour les signatures électroniques, reconnaissant uniquement la validité des signatures électroniques avancées pour les contrats commerciaux électroniques. L'utilisation de signatures électroniques avancées pour les entreprises a été introduite au Kenya par la loi de 2020 portant modification du droit commercial, qui modifiait les statuts liés aux entreprises, y compris la loi sur le droit des contrats prévoyant désormais l'utilisation de signatures électroniques avancées contraignantes en cas de litige. Les signatures électroniques avancées ne sont considérées comme valables que si elles sont émises par un prestataire de services certifié, agréé par l'Autorité des communications du Kenya et seulement pour les contrats commerciaux. En outre, si un document contient une signature électronique avancée étrangère, les fournisseurs de signatures électroniques, par exemple DocuSign, peuvent être reconnus localement à condition qu'ils soient agréés par leurs autorités nationales et respectent la législation du Kenya et les normes internationales[34].

Sénégal

À l'image du Kenya, le Sénégal applique une stratégie prescriptive pour les signatures électroniques. Plus spécifiquement, en accord avec la loi type de 1996 de la CNUDCI sur le commerce électronique, le droit national du Sénégal permet l'utilisation des signatures électroniques comme une méthode d'authentification, adoptant la neutralité technologique et considérant comme équivalents les documents à signature électronique et ceux à signature manuscrite[35]. Afin d'empêcher les activités frauduleuses et de conserver la confiance des utilisateurs, le Sénégal n'autorise juridiquement que certaines entreprises[36] à valider les signatures électroniques, ce qui complique encore le processus d'authentification[37]. Comme illustré ci-dessus, les lois nationales du Sénégal sur les signatures électroniques divergent de celles du Nigeria et de l'Afrique du Sud.

3.1.2 Protection du consommateur en ligne

La protection du consommateur dans le cadre des transactions en ligne est une autre facette majeure de la réglementation des transactions électroniques. Pour que les consommateurs puissent correctement effectuer et participer à des transactions en ligne, il convient de traiter les aspects socioéconomiques du commerce en ligne[38]. Il est nécessaire de s'assurer que les consommateurs sont protégés contre les menaces en ligne, par exemple les attaques par des virus, les spams, la fraude à la carte, les produits défectueux, les déclarations trompeuses, etc.[39] Actuellement, la protection du consommateur en ligne est réglementée en fonction de différentes approches. Certains gouvernements se sont appuyés sur l'autorégulation de l'industrie, développant des méthodes assurant la sécurité du consommateur lors de

transactions en ligne[40]. D'autres gouvernements ont élaboré une réglementation explicite, y compris des dispositions à l'égard des retours, de la sécurité des consommateurs, de la responsabilité des fournisseurs et des mécanismes de recours inadéquats lors de violations des droits des consommateurs[41]. Plus particulièrement pour les accords commerciaux, plusieurs accords régionaux tels que l'accord de libre-échange (ALE) Colombie-Triangle du Nord et l'accord de libre-échange Canada-Honduras contiennent des dispositions « non contraignantes », où les pays reconnaissent l'importance de mesures transparentes et efficaces et, par conséquent, s'attachent à coopérer pour échanger des informations sur les stratégies réglementaires[42]. D'autres accords commerciaux, notamment l'ALE Association des nations de l'Asie du Sud-Est (ANASE)–Australie–Nouvelle-Zélande, emploient un ton plus ferme, les pays s'engageant à fournir le même niveau de protection du consommateur en ligne et hors ligne[43].

Stratégies régionales vis-à-vis de la protection du consommateur en ligne

À l'échelle régionale, la loi type sur les transactions électroniques et le commerce électronique de la Communauté de développement de l'Afrique australe (CDAA) établit des lignes directrices qui définissent les obligations d'un fournisseur à donner aux clients, par exemple, des informations complètes sur le bien ou le service, ainsi que sur le système de paiement et les conditions de l'accord, en plus d'accorder un droit d'annulation aux clients[44]. Pour l'ensemble de la région, 25 des 54 pays disposent d'une forme de législation quant à la protection du consommateur en ligne et quatre ont une législation préliminaire, selon la CNUCED. Comme illustré ci-dessous, cette étude montre que seuls l'Afrique du Sud et le Sénégal prévoient une réglementation spécifique sur la protection du consommateur en ligne, tandis que le Nigeria et le Kenya n'en ont pas à l'heure actuelle. Ceci indique que le développement de la réglementation sur la protection du consommateur en ligne n'en est qu'à ses débuts. Toutefois, selon une étude menée auprès d'entreprises africaines, la protection du consommateur en ligne a été identifiée comme un obstacle majeur au commerce électronique. De plus, des préoccupations ont été exprimées vis-à-vis du renforcement de la confiance des consommateurs et de la mise à disposition de services alternatifs de résolution des conflits, à la fois à l'échelle nationale et à sur le plan transfrontalier[45]. Ainsi, dans le contexte des négociations de Phase II de la ZLECAf et parce que nombre de pays sont encore en train de développer leurs stratégies réglementaires quant à cet enjeu, il est important que les pays considèrent s'il serait plus judicieux pour leurs intérêts de s'accorder sur des engagements solides à l'égard de la protection du consommateur en ligne dans un accord commercial. Tout en déterminant la meilleure voie à suivre, les membres de la ZLECAf doivent examiner s'ils disposent des capacités et des ressources individuelles nécessaires pour implémenter et faire respecter les engagements éventuellement conclus pour protéger le consommateur en ligne.

Afrique du Sud

L'Afrique du Sud prévoit une réglementation explicite sur la protection du consommateur en ligne dans ses lois nationales, visant une sécurité juridique pour les transactions en ligne. En plus d'obliger les fournisseurs en ligne vendant ou louant des biens ou des services en ligne à

partager toutes les informations pertinentes les concernant avec le consommateur, l'ECTA de l'Afrique du Sud applique la loi type sur les transactions électroniques et le commerce électronique de la CDAA et établit également les conditions de l'offre et de l'acceptation d'un contrat électronique[46]. De plus, l'ECTA définit comme un acte délictueux l'envoi de communications commerciales non sollicitées (spams) aux consommateurs sans leur donner la possibilité de se désabonner[47]. Des accusations et des sanctions pénales peuvent aussi être prononcées si un consommateur continue à recevoir des spams alors qu'il a déjà transmis une notification indiquant qu'il ne souhaite plus recevoir d'e-mails. Lorsqu'un consommateur demande à savoir comment ses informations ont été obtenues, les expéditeurs ont l'obligation de fournir ces détails[48].

Nigeria

La loi sur la protection du consommateur en ligne étant inachevée au Nigeria, la position du pays à cet égard n'est pas claire à l'heure actuelle. Bien que la loi fédérale de 2019 du Nigeria sur la concurrence et la protection des consommateurs (loi FCCP, Federal Competition and Consumer Protection Act) protège plusieurs droits des consommateurs, y compris celui d'obtenir des informations présentées dans un langage simple et compréhensible, de pouvoir examiner des biens, de renvoyer des achats, etc., elle ne mentionne pas explicitement les produits et les services en ligne[49]. Cela signifie que la loi FCCP est ambiguë par rapport aux transactions en ligne. Cependant, en 2018, le Conseil de protection des consommateurs a développé des principes visant à traiter les questions des transactions en ligne et du commerce électronique, bien qu'il n'y ait eu aucune mise à jour sur l'implémentation des principes[50]. Ces principes reconnaissent entre autres l'importance de divulguer l'intégralité de toute condition transactionnelle[51].

Kenya

Si pour l'heure le Kenya ne dispose pas d'une législation nationale spécifique quant à la protection du consommateur en ligne, la loi kenyane de 2012 de protection du consommateur (loi KCP, Kenyan Consumer Protection Act), garantissant la protection des droits des consommateurs, fait référence aux situations dans lesquelles un consommateur est protégé dans le cadre d'une « convention électronique »[52]. Conformément à la section d'interprétation de la loi KCP, une convention électronique désigne une « convention de consommation formée par des communications Internet textuelles »[53], qui peuvent donc être interprétées comme incluant les transactions en ligne. Au regard de la loi KCP, avant de conclure un accord en ligne, le consommateur doit être informé de toutes les conditions associées, y compris les circonstances dans lesquelles il peut annuler l'accord[54]. Cependant, la loi KCP ne régulant pas directement les transactions en ligne, elle n'aborde pas les questions importantes comme les spams, l'utilisation abusive des données et le renvoi de biens ou de services. On ignore si le manque de législation adéquate quant à la protection du consommateur en ligne indique que le Kenya travaille actuellement à une législation spécifique dans ce secteur ou s'oriente vers une autorégulation de l'industrie. Dans le premier cas, le pays doit considérer la manière dont ses homologues de la ZLECAf ont réglementé la protection du consommateur en ligne et si des mesures similaires fonctionneraient correctement dans le système juridique du Kenya, offrant la confiance requise au consommateur en ligne au Kenya et dans toute la région.

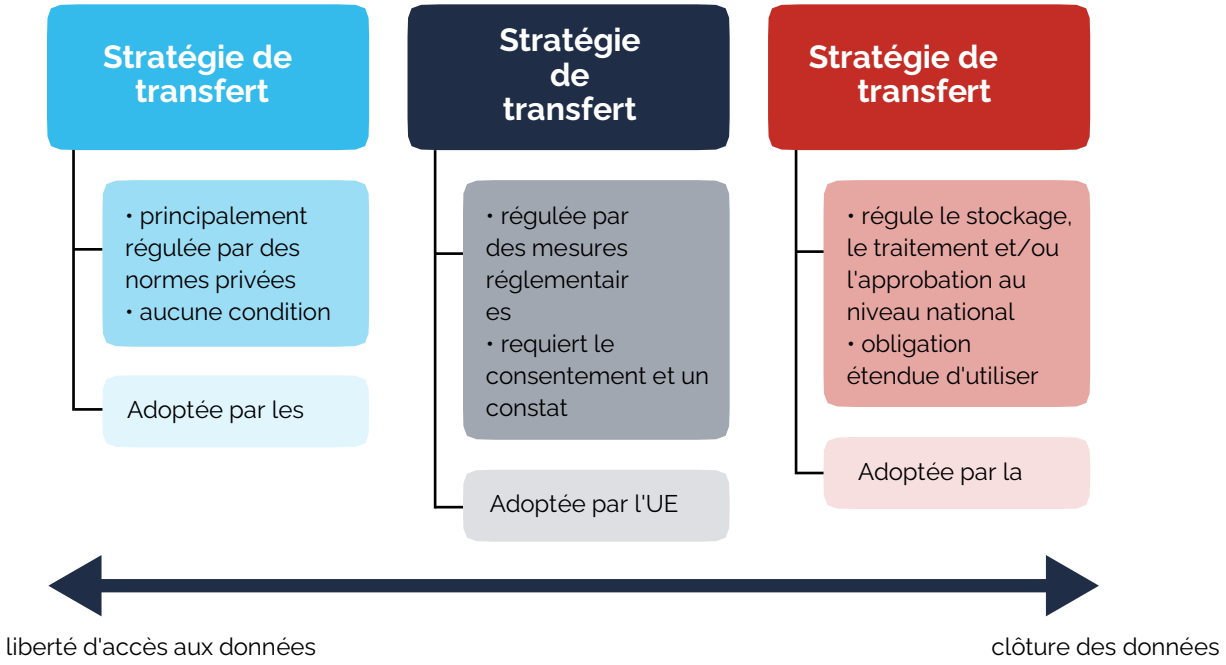
Sénégal

En réglementant explicitement la protection du consommateur en ligne, le Sénégal veut équilibrer les droits des consommateurs en ligne et les obligations des fournisseurs en ligne et applique des règles assurant la sécurité et la responsabilisation des plateformes de commerce électronique. Par exemple, le décret de 2008 du Sénégal relatif au commerce électronique stipule des obligations telles que le devoir d'information, en vertu duquel le fournisseur en ligne doit divulguer toutes les informations pertinentes le concernant, par exemple, ses coordonnées, les informations pertinentes sur le bien ou le service, les modes de paiement, les conditions de garantie, etc.[55] Le décret relatif au commerce électronique établit des droits tels que le droit de rétractation, selon lequel un consommateur ayant conclu un contrat avec un fournisseur en ligne peut se rétracter dans les délais prévus par le contrat sans s'exposer à des frais[56]. La loi protège également les fournisseurs en ligne contre les abus en autorisant uniquement l'application du droit de rétractation lorsque le contrat de vente en ligne prévoit une période d'essai des biens ou du service[57]. Ainsi, il incombe au consommateur de s'assurer que, s'il décide de se rétracter, il renvoie les biens intacts. La loi du Sénégal portant sur la cybercriminalité prévoit aussi des sanctions applicables si les réglementations ci-dessus sont enfreintes.

3.2 Flux de données transfrontaliers, localisation de données et protection des données personnelles

Les flux de données transfrontaliers impliquent le transfert d'informations numériques, publiques ou privées, d'une juridiction à une autre. Compte tenu de la transformation numérique actuelle, c'est un point important, car la production comme le commerce s'appuient de plus en plus sur le stockage, le déplacement et l'utilisation des informations numériques, un processus encore accéléré par la pandémie de COVID-19[58]. Pour équilibrer les gains économiques potentiels des flux de données et les objectifs des politiques nationales, les pays ont tenté de définir la meilleure manière de réglementer les flux de données transfrontaliers, y compris dans des accords commerciaux[59]. Quelques stratégies de réglementation des flux de données transfrontaliers commencent à émerger, comme l'indique la figure 2 ci-dessous.

Figure 2 : Stratégies vis-à-vis du transfert de données[61]



La première stratégie est le « transfert ouvert », principalement utilisé aux États-Unis[62]. Cette approche permet au secteur privé de fixer les normes et de s'autoréguler, empêchant la plupart des restrictions sur le transfert de données transfrontalier et créant un environnement favorable à un flux de données libre plutôt qu'à la protection ou à la confidentialité du consommateur[63]. Bien qu'elle encourage l'innovation, cette stratégie a été critiquée pour son incapacité à protéger correctement les données des consommateurs et le fait qu'elle néglige leur confidentialité.

A contrario, la stratégie de « transfert conditionnel », également appelée stratégie de « priorité à la confidentialité », utilisée par l'UE, privilégie la confidentialité individuelle. Les données personnelles ne peuvent être transférées que lorsque les pays tiers ont obtenu un constat d'adéquation garantissant les mêmes niveaux de protection des données[64]. Si cette approche traite la question de la confidentialité, les critiques font valoir qu'elle enfreint la clause de la nation la plus favorisée du fait de ses décisions par rapport à l'adéquation, qui accordent de façon subjective un régime spécial à certains pays et pas à d'autres. En outre, elle engendre un système onéreux sur lequel les pays en développement et moins développés doivent essayer de s'aligner[65].

La stratégie de « transfert limité », souvent appelée stratégie de « localisation des données », est utilisée à divers degrés, essentiellement par les pays en développement, y compris plusieurs pays d'Afrique comme le Nigeria et le Kenya où le cadre réglementaire se compose d'éléments de cette stratégie[66]. Les mesures de localisation des données impliquent généralement l'obligation de collecter, de traiter et de stocker les données avant de procéder à un transfert et un usage transfrontaliers[67]. L'éventail des mesures de localisation des données s'étend des plus restrictives, c'est-à-dire celles requérant de remplir plusieurs conditions avant de transférer les données (par exemple, traiter et stocker les données localement), aux moins restrictives, celles limitant uniquement le mouvement des données de sorte qu'une entreprise locale décide où stocker et traiter les données[68].

Les lois de localisation des données peuvent être utiles pour atteindre divers objectifs de politiques, notamment la protection de droits fondamentaux tels que le droit à la confidentialité, la promotion d'une croissance et d'une innovation inclusives à l'échelle nationale[69], le respect des obligations réglementaires impliquant la garantie d'accès aux données à des fins de contrôle et la sécurité nationale, selon le principe que la localisation des données réduit les risques d'accès non autorisé, etc.[70] De plus, comme le font remarquer Foster et Azmeh, les mesures de localisation peuvent servir de stratégie d'industrialisation moderne, facilitant l'inclusion d'économies en développement dans des réseaux de production complexes et donnant la possibilité aux pays en développement de rattraper leur retard[71]. Selon l'Institut de la finance internationale (IFI), bien qu'il soit louable que les pays ciblent les objectifs susmentionnés, ils ont tort d'attribuer leur concrétisation à des mesures de localisation des données[72], car cela indique une incompréhension fondamentale sur la manière dont les données prennent de la valeur, et quand. L'IFI soutient que les mesures de localisation des données compromettent la croissance commerciale et économique en limitant la libre circulation des données, ralentissant ainsi l'écosystème numérique[73].

Stratégies régionales vis-à-vis des flux de données transfrontaliers

À l'échelle régionale, la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo) est l'outil présentant le plus grand potentiel d'harmonisation des réglementations dans des secteurs tels que les flux de données transfrontaliers et la protection et la confidentialité des données personnelles pour tous les États membres[74]. Empruntant des éléments juridiques à la directive de l'UE sur la protection des données (remplacée par le RGPD), la Convention de Malabo applique la stratégie de transfert conditionnel mentionné ci-dessus, où le transfert de données personnelles n'est autorisé qu'après un constat d'adéquation et le consentement du sujet des données[75]. Mais au moment de la rédaction de ce rapport, seuls huit pays avaient ratifié la convention, le Sénégal étant le seul à l'avoir fait parmi les quatre pays analysés dans le présent document[76].

D'autres efforts d'harmonisation du système réglementaire pour les flux de données transfrontaliers ont commencé à voir le jour dans les communautés économiques régionales (CER). En 2008, par exemple, la Communauté d'Afrique de l'Est (CAE) a lancé le Cadre de la CAE pour les Phases I et II de la cyberlégislation (le cadre de la CAE), qui traite plusieurs enjeux de la cyberlégislation, y compris la protection des données. Cependant, le cadre de la CAE ne prévoit pas d'orientation spécifique sur la stratégie réglementaire que ses membres doivent adopter. Elle stipule que ceux-ci doivent respecter les « principes de bonnes pratiques » vis-à-vis de tous les aspects des flux de données transfrontaliers[77]. À titre de comparaison, l'Acte additionnel de 2010 de la CEDEAO relatif à la protection des données à caractère personnel (Acte additionnel de la CEDEAO), spécifie le contenu requis pour les lois sur la confidentialité des données et exige de chaque État membre qu'il mette en place une autorité de protection des données. L'Acte additionnel de la CEDEAO est juridiquement contraignant mais n'est applicable que lorsque les États membres établissent des cadres de protection des données. En avril 2021, si 11 États membres de la CEDEAO disposaient de lois sur la protection des données, seuls quatre avaient

promulgué une législation sur la protection des données après la conclusion de l'Acte additionnel de la CEDEAO, le Nigeria ne figurant pas parmi eux[78]. En 2013, la CDAA a également publié une loi non contraignante sous forme d'une loi type sur la protection des données, qui prévoit des lignes directrices sur la promulgation de lois de confidentialité[79] mais n'est pas contraignante pour les membres de la CDAA.

Il est intéressant de noter que les trois instruments réglementaires régionaux susmentionnés contiennent des éléments similaires au RGPD de l'UE concernant la confidentialité. Toutefois, comme nous le verrons ci-dessous,
les stratégies réglementaires nationales adoptées sur les flux de données transfrontaliers par les pays cibles de ce rapport semblent diverger de celles adoptées par leurs communautés économiques régionales respectives. Par exemple, dans le cas du Nigeria, il existe une contradiction entre les mesures de localisation de données du pays et ses engagements régionaux en vertu de l'Acte additionnel de la CEDEAO, qui applique une stratégie de transfert conditionnel. Cette divergence illustre toutes les difficultés de la réglementation et de l'implémentation des flux de données transfrontaliers au niveau des communautés économiques régionales. Ceci peut venir du fait que les pays membres présentent diverses valeurs socioculturelles et cultures juridiques[80].

C'est pourquoi, avec le protocole sur le commerce électronique de la ZLECAf, les pays ont l'opportunité de créer une législation apte à concrétiser l'équilibre délicat entre leurs intérêts et priorités nationaux et des lois bénéfiques sur le plan économique[81]. C'est extrêmement important pour le continent africain, car il génère d'énormes quantités de données, donnant la possibilité aux pays d'obtenir des gains économiques considérables du commerce basé sur les données[82]. Des variations minimes sont essentielles au niveau de la législation des flux de données transfrontaliers dans la ZLECAf, car elles permettront aux entreprises (en particulier les microentreprises et les PME, qui constituent la plupart des entreprises du continent) de satisfaire leurs obligations légales sans subir de coûts de conformité élevés. Cependant, il est important que les pays considèrent les répercussions de chaque stratégie réglementaire et s'ils disposent des ressources requises pour l'implémentation[83]. En plus de définir quelle stratégie sert au mieux leurs intérêts, les membres de la ZLECAf pourront examiner si une stratégie réglementaire unique satisferait les intérêts sociaux et économiques de tous les membres de la ZLECAf, compte tenu de leurs différences culturelles et économiques. En outre, les membres de la ZLECAf pourront déterminer comment concrétiser cette harmonisation, ou interopérabilité, s'ils se tournent vers cette solution. Toutes ces considérations comptent, car il existe actuellement une polarisation entre pays développés et en développement à l'égard de la stratégie adéquate de réglementation des flux de données transfrontaliers. De plus, les pays africains peuvent être poussés à adhérer à certaines stratégies lors des négociations du protocole de la ZLECAf sur le commerce électronique.

Afrique du Sud

Dans son approche des flux de données transfrontaliers, l'Afrique du Sud associe des éléments du RGPD de l'UE et des règles de localisation des données moins restrictives. Conformément à la loi de 2013 sur la protection des renseignements personnels (loi POPI)[84], le principal instrument législatif du pays quant à la protection et au transfert des données, l'Afrique du Sud a adopté une stratégie de transfert conditionnel. Ceci implique que pour l'Afrique du Sud, les données personnelles peuvent uniquement être transférées vers un pays tiers où :

(i) le destinataire est soumis à une loi, des règles d'entreprise contraignantes ou un accord contraignant fournissant un niveau de protection adéquat, défendant des principes de traitement raisonnable des informations essentiellement similaires aux conditions d'un traitement licite stipulé par la loi POPI ;

(ii) le sujet des données consent au transfert ;

(iii) le transfert est nécessaire à l'exécution d'un contrat entre le sujet des données et la partie responsable ou à l'implémentation de mesures précontractuelles prises à la demande du sujet des données ;

(iv) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt du sujet des données entre la partie responsable et un tiers ; ou

(v) le transfert s'effectue dans l'intérêt du sujet des données et il est difficile sur le plan pratique d'obtenir son consentement à cet égard, et s'il était possible de le lui demander, le sujet accepterait probablement.

À l'évidence, à l'instar du RGPD, de la loi type de la CDAA sur la protection des données et de la Convention de Malabo, la loi POPI confère des droits au sujet des données et oblige les contrôleurs de données à s'assurer que lors du transfert transfrontalier de données personnelles, le pays destinataire offre un niveau de protection des données adéquat. De plus, comme illustré ci-après, ces éléments de la loi POPI ont aussi été adoptés par le Kenya et le Sénégal.

Toutefois, si la loi POPI suit en majeure partie le RGPD de l'UE[85], la version préliminaire de la politique nationale de l'Afrique du Sud sur les données et le cloud (publiée pour examen public en avril 2021) propose d'imposer davantage de politiques de localisation des données aux flux de données transfrontaliers[86]. Celles-ci incluent des obligations telles que le traitement et le stockage au sein des frontières de l'Afrique du Sud de toutes les données identifiées ou classées comme des informations sensibles, ainsi que le traitement comme propriété de l'Afrique du Sud des données générées au sein de ses frontières, même par une entreprise étrangère[87]. Les critiques de cette version provisoire ont fait valoir que, même si le gouvernement tente ainsi d'obtenir le contrôle des données d'origine locale, les mesures très strictes (qui dévient du cadre réglementaire instauré par la loi POPI) proposées pour la localisation des données risquent de nuire à la protection de la confidentialité et d'étouffer la concurrence dans le secteur du cloud[88]. De plus, si l'Afrique du Sud adoptait ces mesures de localisation des données, elles seraient contraires à la loi type de la CDAA et à la Convention de Malabo, bien qu'il convienne de noter que la loi type de la CDAA n'est pas contraignante pour l'Afrique du Sud et que cette dernière n'a pas encore signé ou ratifié la Convention de Malabo.

Par conséquent, en tenant compte de l'ensemble des réglementations de l'Afrique du Sud sur les flux de données transfrontaliers, on peut soutenir que le pays est en train de développer une stratégie hybride privilégiant la confidentialité des sujets des données, mais semble également s'intéresser à la promotion de la souveraineté des données.

Nigeria

Comme l'Afrique du Sud, le Nigeria applique une stratégie hybride pour réglementer les flux de données transfrontaliers, mais il associe des éléments de confidentialité des données similaires au RGPD via une stratégie de transfert conditionnel, avec des règles de localisation des données relativement plus strictes.

Le Règlement nigérian de 2019 sur la protection des données (NDPR), qui est aussi sa réglementation actuelle, exige que tout transfert de données personnelles vers des pays étrangers s'effectue avec l'approbation de l'Agence nationale de développement des technologies de l'information (NITDA) et sous la supervision du procureur général[89]. Ces mesures visent à s'assurer que l'adéquation législative du pays destinataire fournit le même niveau de protection que le Nigeria. Il existe cependant quelques exceptions prévoyant le transfert sans approbation des données. Elles incluent les situations où : les sujets des données ont explicitement consenti au transfert, le transfert est nécessaire à l'exécution ou à la conclusion d'un contrat entre le sujet des données et une autre partie ou lorsque le transfert sert l'intérêt public[90]. De plus, la loi prévoit des sanctions susceptibles d'être infligées aux contrôleurs des données en cas de violation de ces règles, selon le nombre de sujets de données légaux qu'ils traitent[91]. La NITDA est responsable de l'application des dispositions du NDPR, ainsi que de l'enregistrement et de l'agrément des Organisations de conformité en matière de protection des données chargées de surveiller, de vérifier et de dispenser en son nom des formations et des consultations sur la conformité en matière de protection des données. Par ailleurs, le NDPR garantit un niveau élevé de confidentialité des données aux entreprises et aux citoyens du Nigeria[92]. Fait intéressant, le NDPR n'étant pas une loi du Parlement, des questions ont été soulevées à l'égard de son efficacité et de son applicabilité, ainsi que de sa portée, suffisante ou non[93]. En raison de ces lacunes, le gouvernement fédéral a publié en 2020 à des fins de commentaires un projet de loi sur la protection des données devant succéder au NDPR. Le projet de loi, similaire à la loi POPI de l'Afrique du Sud, prévoit l'obligation d'obtenir le consentement du sujet des données, un motif légitime et explicite au traitement des données personnelles, une décision d'adéquation pour d'autres juridictions, etc. La NTIDA a également publié la Politique du Nigeria sur le cloud computing, qui promeut les transferts de données transfrontaliers mais exige aussi que, si des fournisseurs de services cloud concluent un contrat avec des institutions nationales nigérianes, cela s'effectue à condition que les données soient stockées dans une juridiction dont le niveau de protection des données est équivalent à celui du Nigeria[94].

Concernant les règles de localisation des données, les Directives contraignantes pour le développement de contenu nigérian dans les technologies de l'information et de la communication (les Directives TIC), également appliquées par la NTIDA,
– exigent que les entreprises de télécommunication hébergent toutes les données d'abonnés et de consommateurs au Nigeria et que les entreprises de gestion des données et des informations hébergent elles aussi les données nationales/gouvernementales localement[95]. L'objectif est de stimuler et d'accroître l'innovation locale dans les produits et les services des technologies de l'information pour le développement de l'industrie des TIC. Indépendamment, les Directives de 2011 de la Banque centrale du Nigeria sur les services d'acceptation des cartes dans les points de vente (PDV) stipulent que l'infrastructure destinée au traitement du paiement doit se trouver dans le pays. Toutes les transactions nationales via des points de vente et des guichets automatiques bancaires (GAB) doivent être traitées par des commutateurs locaux et il est interdit

de les acheminer hors du pays pour les traiter[96].

Si des règles de localisation des données peuvent s'avérer bénéfiques, le Nigeria doit considérer que lorsque ces règles sont appliquées avec rigueur elles peuvent se révéler protectionnistes, entraver le commerce transfrontalier lié aux données et servir d'obstacle non tarifaire. Ainsi, des règles strictes de localisation des données risquent d'empêcher de profiter pleinement des avantages économiques associés au commerce basé sur les données. Cet aspect est très important, car l'article 15 du protocole de la ZLECAf sur le commerce des services autorise uniquement l'application de règles de localisation des données lorsque celles-ci ne constituent pas une « discrimination arbitraire et injustifiable »[97]. Le Nigeria doit donc, tout comme l'Afrique du Sud, considérer l'incompatibilité éventuelle entre des règles strictes de localisation des données et ses engagements régionaux en vertu de l'Acte additionnel de la CEDEAO (et de la Convention de Malabo, s'il la ratifie), et si, à long terme, de telles mesures lui permettraient de profiter pleinement des avantages économiques qu'il peut tirer du commerce basé sur les données. De surcroît, en continuant à imposer des règles strictes de localisation des données, le Nigeria risque de rencontrer des difficultés lors de négociations de dispositions numériques avec des pays défendant la libéralisation des flux de données, par exemple les États-Unis.

Kenya

À l'instar de l'Afrique du Sud et du Nigeria, le Kenya applique des lois de protection des données comportant des obligations de localisation. La loi du Kenya de 2019 sur la protection des données (KDPA) est son instrument juridique majeur à l'égard du transfert transfrontalier des données. Il suit, dans une plus large mesure, le RGPD de l'UE. Le KDPA autorise uniquement le transfert transfrontalier des données lorsque le contrôleur ou le processeur des données prouve au préalable au Commissaire à la protection des données que des mesures suffisantes de protection de la sécurité et de la confidentialité sont en place[98]. Ceci inclut l'obligation pour le processeur/contrôleur des données d'assurer que, lorsque le transfert des données est nécessaire[99], le pays destinataire dispose de lois de protection des données équivalentes et que le sujet des données (après avoir été pleinement informé d'éventuels risques) a consenti au transfert transfrontalier de ses données personnelles[100].

Toutefois, la section 50 du KDPA introduit certaines mesures de localisation des données. Selon cette disposition du KDPA, le secrétaire du Cabinet a la capacité de limiter le traitement d'autres types de données personnelles ou publiques hors du Kenya[101]. De plus, les projets de réglementations de 2021 du Kenya pour la protection des données stipulent que lorsque les données sont traitées pour un service public, y compris pour faciliter l'accès à l'éducation et l'administration fiscale, ceci doit s'effectuer via un serveur et un centre de données situés au Kenya[102]. Il est donc interdit aux processeurs/collecteurs de données de traiter des données personnelles destinées à un service public hors du Kenya ou avec des serveurs/centres de données étrangers. Ces réglementations soulignent la priorité du Kenya, assurer la confidentialité des sujets de données, tout en indiquant (comme sa politique sur les TIC) la volonté d'accroître la capacité du pays à stocker et à utiliser ses propres données, y compris grâce à la construction de centres de données régionaux et centraux. Contrairement au Nigeria, dont les règles de localisation des données reposent sur un intérêt économique, les objectifs du Kenya semblent davantage motivés par la nécessité de fournir une confidentialité maximale à ses sujets de

données.

En plus de ses lois nationales, le Kenya a conclu un accord de partenariat économique avec le Royaume-Uni dont les lignes directrices stipulent que les données personnelles ne peuvent être échangées que lorsque le pays destinataire accepte de garantir un niveau de protection des données équivalent à celui du pays émetteur[103]. Ceci crée donc un besoin d'adéquation préalable au transfert, ce à quoi les réglementations nationales du Kenya font également écho. Actuellement, le Kenya négocie l'ALE États-Unis–Kenya, dont les objectifs de négociation indiquent, selon le Bureau du représentant américain au Commerce, que les États-Unis veulent réduire au maximum les obstacles aux flux de données transfrontaliers entre les deux pays[104]. Les mesures de localisation des données du Kenya risquent fort de susciter la discorde à ce sujet entre le pays et les États-Unis.

Sénégal

À l'inverse de l'Afrique du Sud, du Kenya et du Nigeria, le Sénégal semble opter pour une stratégie de transfert conditionnel sans mesures de localisation des données. Bien qu'il comporte encore des lacunes réglementaires, d'implémentation et d'application, le système national de protection des données du Sénégal se rapproche nettement du RGPD de l'UE en privilégiant la protection du détenteur des données. La loi du Sénégal de 2008 sur la protection des données (Data Protection Act, DPA de 2008), actuellement en vigueur, a pour modèle l'Acte additionnel de la CEDEAO, lui-même fortement influencé par la directive de l'UE sur la protection des données. Conformément à l'Acte additionnel de la CEDEAO, la loi de 2008 du Sénégal définit les droits fondamentaux des sujets des données, par exemple l'obligation de considérer le traitement des données personnelles comme légitime uniquement lorsque le détenteur/sujet des données consent au traitement de ses données[105]. La collecte et le traitement des données doivent être justifiés par des motifs légitimes, explicites et spécifiques. Tout traitement hors du cadre de ces objectifs est interdit[106].

À l'heure actuelle, le Sénégal envisage d'adopter une nouvelle loi sur la protection des données. Une fois entré en vigueur, le projet de loi de 2019 sur la protection des données personnelles proposé par le Sénégal accordera davantage de droits et de protections au détenteur des données. Par exemple, le projet de loi prévoit une définition plus étroite du « consentement », exigeant que le détenteur des données autorise clairement l'utilisation de ses données personnelles par une action affirmative[107]. Le détenteur des données pourra également retirer son consentement au traitement de ses données quand il le souhaite. En outre, contrairement au DPA de 2008, le projet de loi de 2019 obligera les sous-traitants tiers à respecter la loi[108].

Tout comme l'approche de l'UE, le Sénégal exige systématiquement que tout flux de données transfrontalier s'effectue avec des juridictions garantissant le même niveau de confidentialité et de protection suffisantes via leurs lois[109]. Lorsque ces sécurités n'existent pas, le consentement du détenteur/sujet des données est nécessaire. Mais pour l'heure, le Sénégal n'a pas de système accordant des ententes d'adéquation aux juridictions disposant de régulations de protection des données similaires ou satisfaisantes[110]. Ceci suggère que les entreprises de traitement des données doivent peut-être demander une autorisation pour le transfert individuel de données dans d'autres juridictions, accroissant la responsabilité de la Commission de protection des données quant au respect de la conformité. Alors que le manque d'ententes

d'adéquation suscite déjà des problèmes pour le Sénégal, le transfert transfrontalier des données risque d'accentuer ces difficultés si des pays s'accordent dans le cadre de la ZLECAf sur d'autres normes d'adéquation que celles du Sénégal. C'est un point particulièrement pertinent, car le Sénégal a signé la Convention n°108 de l'UE privilégiant le « droit à la confidentialité lors d'échanges de données personnelles » et limite la libre-circulation des données lorsque la législation de protection des données d'une juridiction contourne la Convention.

3.3 Accès au code source et transfert de technologie

À l'ère numérique, la divulgation obligatoire du code source et des algorithmes est l'une des méthodes employées par les décideurs pour faciliter le transfert de technologies numériques à des fins de développement. Le code source désigne « un ensemble d'instructions saisies dans un ordinateur, traitées et exécutées pour [...] faire fonctionner des logiciels de l'ordinateur »[113]. Grâce au partage et à l'examen des codes source, il est possible de développer de nouvelles techniques de programmation et d'améliorer les logiciels[114]. Plus précisément, la circulation du savoir via la divulgation du code source par des entreprises et des pays avancés sur le plan technologique crée des opportunités d'innovation, de compétitivité et d'amélioration des compétences[115].

L'accord de l'OMC sur les aspects des droits de propriété intellectuelle qui touchent au commerce (accord ADPIC)[116] a posé les bases du transfert de technologie en obligeant les pays développés à inciter au transfert de technologie[117]. Mais l'accord ADPIC ne contient aucune disposition spécifique quant à l'accès au code source. Bien que le code source puisse être protégé par des brevets, des secrets industriels et/ou des droits d'auteurs, l'accord ADPIC n'interdit pas explicitement aux pays de demander la divulgation des codes sources d'entreprises étrangères. Par conséquent, en réponse à cette préoccupation, plusieurs pays tels que les États-Unis, Singapour et l'UE prônent l'inclusion de dispositions sur la propriété intellectuelle (PI) interdisant la divulgation obligatoire du code source et des algorithmes dans des accords commerciaux[118].

Les pays développés, par exemple les États-Unis et l'UE, soutiennent que l'obligation de divulguer les codes sources et les algorithmes sert d'obstacle à l'accès au marché et au commerce[119]. C'est pourquoi ces pays insistent sur l'interdiction impérative de la divulgation du code source. Certaines critiques affirment également que la véritable raison d'être de l'interdiction de la divulgation obligatoire du code source et des algorithmes repose en grande partie sur le besoin d'aider les entreprises à conserver un avantage concurrentiel, ouvrant l'accès au marché à leurs produits intégrant une technologie tout en protégeant leur PI[120]. Par exemple, l'interdiction stipulée par l'ACEUM vise à protéger la PI et l'avantage concurrentiel de ses entreprises en empêchant les gouvernements d'instaurer la divulgation d'informations de cryptographie, algorithmes compris, comme condition préalable à l'accès au marché. De même, l'ALE Royaume-Uni–Japon interdit la divulgation obligatoire par les gouvernements du code source, des logiciels et des algorithmes exprimés dans les logiciels. Les partisans du partage du code source soutiennent que les pays développés protègent leur avantage concurrentiel en

contrôlant le développement technologique, étant donné qu'ils ont déjà bénéficié du partage du code source lors de la première phase de la révolution numérique, lorsque celui-ci n'était pas protégé par les lois de PI.

Mais le code source fait partie intégrante de l'innovation et du développement de technologies numériques. Interdire le partage du code source risque d'entraver le transfert de technologie, limitant ainsi l'accès au savoir et la capacité d'un pays à apprendre par imitation, ainsi qu'à innover, élaborant des modèles distincts dans une chaîne de valeur de données mondiale[124]. Ce défi est encore plus grand pour les pays africains souhaitant tirer parti des opportunités offertes par les technologies numériques pour le développement économique. Qui plus est, les algorithmes soulevant également des inquiétudes au niveau des politiques publiques, telles que la discrimination, le manque d'équité, la transparence et la responsabilisation[125], les défenseurs de l'éthique en matière d'intelligence artificielle (IA) soutiennent que les algorithmes doivent être suffisamment transparents pour être examinés, surtout lorsqu'ils éclairent des décisions aux répercussions discutables ou négatives[126]. Par conséquent, la politique de PI doit être adaptée au contexte économique et social, basée sur des preuves et éclairée par des priorités de politique et de développement. Adopter une approche exclusivement maximaliste, comme le proposent certaines instances, sans exceptions et limitations appropriées risque d'empêcher les pays africains de posséder des droits de PI significatifs ou de devenir des acteurs pertinents des marchés numériques[127]. Il est impératif de traiter les problèmes liés au transfert de technologie, aux mesures anticoncurrentielles, aux obstacles à la conformité et à la responsabilisation sur le plan des algorithmes. Il faut aussi formuler les politiques sans enraciner la domination des grandes entreprises aux dépens des plus petites.

Stratégies régionales vis-à-vis de l'accès au code source

À l'échelle régionale, aucune règle spécifique n'a encore été développée quant à la divulgation obligatoire du code source dans le cadre d'institutions telles que l'African Regional Intellectual Property Organization (ARIPO)[128] ou l'Organisation africaine de la propriété intellectuelle (OAPI)[129]. De plus, comme le montre l'analyse ci-après, l'accès au code source étant relativement récent, la plupart des gouvernements africains n'ont pas encore adopté de législation nationale définissant clairement leur position et leurs priorités vis-à-vis de cet enjeu. Plus spécifiquement, pour les quatre pays cibles de ce rapport, le développement d'une réglementation et d'une politique à cet égard s'effectue de diverses manières et à différents rythmes. Par exemple, comme indiqué ci-dessous, alors que les lignes directrices du Nigeria (qui n'ont pas été implémentées) exigent des entreprises multinationales qu'elles divulguent le code source et les algorithmes de tout logiciel déployé dans le pays, la législation de l'Afrique du Sud limite pour l'heure la divulgation obligatoire aux logiciels utilisés par le gouvernement. En comparaison, la législation du Kenya encourage la divulgation du code source mais ne la demande pas spécifiquement, tandis que le Sénégal n'a pas encore de législation à cet égard. Plusieurs stratégies convergent entre les quatre pays quant à leur intérêt pour le transfert de technologie et leur marge d'action vis-à-vis de l'obligation de divulgation du code source. Mais à l'approche des négociations de Phase II de la ZLECAf, les gouvernements doivent se demander s'il peut être prématuré de négocier des dispositions strictes sur la divulgation obligatoire du code source

dans le cadre de la ZLECAf. Il sera donc peut-être judicieux pour les membres de la ZLECAf, à l'heure actuelle, de s'accorder sur une coopération réglementaire tout en définissant quelle stratégie réglementaire répond au mieux aux intérêts économiques et de développement de la région.

Afrique du Sud

La législation nationale de l'Afrique du Sud exige la divulgation obligatoire du code source, bien qu'elle la limite actuellement aux logiciels utilisés par le gouvernement. Selon la politique de l'Afrique du Sud sur l'utilisation de logiciels libres et gratuits par le gouvernement sud-africain, telle qu'adoptée par le ministère de la Fonction et de l'Administration publiques, seuls des logiciels libres (OSS) doivent être utilisés pour les projets gouvernementaux[130]. Si cela s'avère impossible, la politique stipule que des justifications doivent appuyer cette dérogation. Par ailleurs, la politique exige la divulgation du code source de tout logiciel propriétaire utilisé avant l'adoption de la politique en 2006.

En règle générale, l'Afrique du Sud semble favorable au transfert de technologie pour le développement économique, en particulier par rapport aux sciences et à la technologie. Par exemple, la loi de 2008 de l'Afrique du Sud sur les droits de propriété intellectuelle émanant du financement public en matière de recherche et de développement vise à garantir que la PI découlant de la recherche et du développement financés par des fonds publics soit commercialisée et mise à disposition au profit du public sud-africain. Sur cette base, le ministère de la Science et de la Technologie[133] a publié un livre blanc en 2019 pour définir la politique de l'Afrique du Sud en matière de sciences, de technologie et d'innovation, et soutenir davantage le transfert de technologie, y compris la commercialisation de la PI[134].

Nigeria

Les politiques nationales du Nigeria privilégient la divulgation obligatoire du code source et des algorithmes en imposant des exigences de contenu local pour les TIC. Plus précisément, les Directives modifiées pour le développement de contenu nigérian dans les technologies de l'information et de la communication (Directives TIC) prévoient plusieurs lignes directrices pour le traitement du code source. Par exemple, conformément aux directives TIC, à des fins de sécurité nationale, les entreprises multinationales ont l'obligation de fournir des informations vérifiables sur l'origine, la sécurité, la source et le fonctionnement de leurs logiciels avant de les déployer ou de les vendre au Nigeria[135]. De plus, les ministères et les départements gouvernementaux nigérians des trois niveaux de gouvernance (fédéral, étatique et local) doivent assurer la sécurité de tout logiciel utilisé dans le pays, notamment en obtenant et en vérifiant le code source fourni par la société mère du logiciel. Le Nigeria veille également à l'exécution du transfert de technologie en insistant pour que, lorsque le gouvernement doit utiliser un logiciel et aucun développeur de logiciel nigérian local n'est en mesure de le fournir, toute entreprise étrangère fournissant le logiciel travaille avec une entreprise nigériane locale[136]. Les rôles attendus de l'entreprise nigériane locale étant l'installation et l'assistance, le développeur de logiciel étranger est obligé de divulguer les codes source et les algorithmes pour que les entreprises locales puissent remplir leurs obligations. Bien que le Nigeria n'ait pas encore implémenté ces directives TIC, elles constituent un indicateur majeur de la position du pays à ce sujet.

Kenya

À l'heure actuelle, le Kenya n'encourage l'utilisation d'OSS que dans l'administration publique. D'après la politique nationale du Kenya sur les TIC (2019), les gouvernements doivent utiliser des OSS et opter pour cette solution lorsqu'il existe une alternative aux logiciels propriétaires[137]. Tous les logiciels commissionnés par le gouvernement pour le développement doivent voir leur code source divulgué et rendu public de sorte que n'importe quel autre organisme gouvernemental puisse s'en servir[138]. La politique stipule également que le code source de tous les logiciels acquis par le gouvernement sera répertorié par ce dernier dans un guide public.

Sénégal

Si le Sénégal ne semble pas disposer de politiques ou de lois spécifiques quant à la divulgation du code source, l'administration publique sénégalaise a exprimé son intérêt envers la mise en place de politiques pour des OSS gratuits[139].

3.4 Responsabilité des intermédiaires

Des règles concernant la responsabilité des plateformes Internet vis-à-vis du contenu généré par les utilisateurs ont été formulées dans plusieurs accords commerciaux du monde, par exemple États-Unis–Japon et ACEUM. Ces règles établissent si et dans quelle mesure les plateformes Internet servant d'intermédiaires[140] sont légalement responsables de préjudices et de violations des droits en ligne causés par des contenus tiers qu'elles hébergent ou transmettent.

Figure 3 : Stratégies vis-à-vis de la responsabilité des intermédiaires

Connaissance réelle	Notification et retrait	Simple transport	Digital Millennium Copyright Act américain	Convention de Malabo
• Les intermédiaires sont uniquement responsables du contenu dont ils ont connaissance	• Les intermédiaires doivent retirer le contenu dès qu'ils ont connaissance de sa nature illégale	• Les intermédiaires sont protégés si leur rôle était automatique et de nature passive	• Les intermédiaires sont dégagés de toute responsabilité vis-à-vis de contenus illégaux et sont protégés de toute responsabilité pouvant découler d'une tentative de modération de contenu tiers	• Les États membres africains doivent criminaliser l'hébergement, la diffusion et la transmission d'images ou de représentations relevant de la pornographie infantile, ainsi que les contenus de nature raciste ou xénophobe
• Ex. : Australie, Japon, Inde	• Ex. : Nouvelle-Zélande, Royaume-Uni	• Ex. : UE		

Comme le montre la figure 3, les pays ont adopté diverses stratégies vis-à-vis de la responsabilité des intermédiaires. Certains ont adopté une législation reflétant le modèle de la « connaissance réelle », où les intermédiaires sont tenus pour responsables du contenu dont ils ont connaissance. Par exemple, dans leur législation nationale, l'Australie, le Japon et l'Inde ont adopté ce modèle et dégagent les intermédiaires de toute responsabilité lorsqu'ils ignorent la nature du contenu. Ils ne sont tenus pour responsables que s'ils n'ont pas retiré le contenu ou empêché son accès après avoir eu connaissance qu'il enfreignait le droit d'autrui[142]. D'autres pays comme la Nouvelle-Zélande et le Royaume-Uni ont opté pour le modèle « notification et retrait » où, pour ne pas être tenus responsables,
– les intermédiaires doivent retirer tout contenu illicite de leurs plateformes dès qu'il leur est signalé. Même si ce modèle décharge les intermédiaires d'un contrôle proactif et de la vérification de la conformité légale de tous les contenus avant leur publication, les critiques font valoir qu'il incite les plateformes à retirer tout contenu signalé sans forcément chercher à savoir s'il enfreint réellement la loi[143]. Le modèle du « simple transport » est employé par des juridictions telles que l'UE. Il protège les intermédiaires de toute responsabilité lorsque leur activité est de nature automatique et passive, par exemple les services de mise en cache et d'hébergement[144].

Il est intéressant de noter, comme l'indique la figure 3, que les États-Unis utilisent un modèle légèrement différent vis-à-vis de la responsabilité des intermédiaires, incluant des éléments des trois approches[145]. Au regard de la loi américaine, les intermédiaires sont protégés de toute conséquence juridique découlant d'un contenu illégal d'utilisateurs tiers et de toute responsabilité résultant d'une tentative de modération d'un contenu tiers[146]. Cela signifie que les intermédiaires ne peuvent être tenus pour responsables, qu'ils diffusent un contenu tiers illégal ou retirent injustement un contenu tiers dont l'illégalité n'est pas démontrée. Les critiques de cette approche soutiennent qu'elle est trop vaste et protège donc les intermédiaires de toute responsabilité lorsque leurs plateformes entraînent une violation directe ou indirecte des droits d'utilisateurs d'Internet[147]. De surcroît, les États-Unis semblent avoir incité certains de leurs partenaires commerciaux à adopter cette stratégie vis-à-vis de la responsabilité des intermédiaires lors d'accords commerciaux. Par exemple, un langage très proche de la loi américaine dans ce domaine apparaît dans l'accord sur le commerce numérique entre les États-Unis et le Japon, ainsi que dans l'ACEUM[148].

Stratégies régionales vis-à-vis de la responsabilité des intermédiaires

À l'inverse de tous les modèles détaillés ci-dessus, la Convention de Malabo de l'Union africaine a opté pour une approche complètement différente, préconisant le modèle de la « responsabilité des intermédiaires ». Au regard de la Convention de Malabo, les États membres africains doivent criminaliser l'hébergement, la diffusion et la transmission d'images ou de représentations relevant de la pornographie infantile, ainsi que de contenus de nature raciste ou xénophobe[149]. Pour les critiques de la Convention de Malabo, celle-ci est trop stricte et risque d'entraver le commerce numérique et la liberté d'expression en ligne. Il convient également de noter, comme mentionné ci-dessous, que les quatre pays cibles de ce rapport ont adopté des

modèles réglementaires divergeant de la Convention de Malabo. Plus précisément, si l'approche réglementaire de chacun des quatre pays diffère, ils partagent un intérêt commun : ne pas imposer trop de responsabilité à l'intermédiaire, contrairement à la Convention. Néanmoins, indépendamment de cet intérêt similaire, les quatre pays divergent dans leurs stratégies réglementaires. Cela indique clairement toute la complexité de la réglementation du contenu et de la responsabilité des intermédiaires, et qu'il faut donc trouver un équilibre. Même si les « fake news », la désinformation et les discours de haine peuvent menacer les utilisateurs d'Internet, les experts estiment qu'une réglementation du contenu excessivement large ou mal alignée risque elle aussi d'enfreindre les droits des utilisateurs[150]. Par exemple, certains modèles de responsabilité incitent les plateformes à utiliser des outils de filtrage et à adopter des procédures de vérification susceptibles d'enfreindre les droits humains, notamment en censurant l'expression légitime. Alors que les accords commerciaux incluent de plus en plus des dispositions réglementant le contenu Internet et la responsabilité des intermédiaires, les politiques commerciales doivent s'efforcer de trouver un juste milieu entre ces objectifs[151]. Il est donc vital, à l'approche des négociations de Phase II de la ZLECAf, que les pays considèrent soigneusement les répercussions des modèles discutés, eu égard à leurs priorités et intérêts sociaux, politiques et économiques. Les membres de la ZLECAf doivent aussi déterminer si une harmonisation leur permettrait d'atteindre leurs objectifs économiques et de politiques, et si la ZLECAf constitue la meilleure plateforme pour traiter ces enjeux.

Afrique du Sud

Actuellement, la stratégie de l'Afrique du Sud vis-à-vis de la responsabilité des intermédiaires est hybride, associant divers éléments des modèles présentés dans la figure 3. En vertu de la loi de 2002 de l'Afrique du Sud sur les communications et transactions électroniques (loi ECTA), les intermédiaires ne sont dégagés de toute responsabilité que lorsqu'ils ont transmis, mis en cache, stocké ou hébergé du contenu illégal sans avoir connaissance de la nature dudit contenu[152]. Empruntant ici au modèle de « connaissance réelle », la protection est aussi offerte à condition que les intermédiaires ne modifient pas le contenu, ne participent pas à sa création et ne sélectionnent d'aucune manière le destinataire du contenu[153]. Cependant, la loi ECTA inclut également une disposition de « notification et retrait » stipulant que les intermédiaires doivent retirer le contenu, en empêcher l'accès ou cesser la transmission lorsqu'ils sont avertis de sa nature illicite[154]. Mais comme avec le modèle américain, en cas de retrait abusif de contenu, la loi sud-africaine protège les intermédiaires et impute la responsabilité à l'individu qui a envoyé la notification, étant donné qu'il a sciemment déformé les faits[155]. La législation de l'Afrique du Sud diffère de l'approche des États-Unis en stipulant que les intermédiaires ne peuvent bénéficier de ces dispositions de décharge que si ce sont des membres d'un représentant de l'industrie enregistré auprès du ministère des Communications et s'ils adoptent et implémentent le code de conduite de ce représentant. Ainsi, le représentant de l'industrie a la capacité de définir les procédures de retrait spécifiques[156]. Les décideurs sud-africains jugent que ce modèle est le plus efficace, en plus d'être crucial pour accroître la disponibilité publique des services Internet[157]. Comme mentionné ci-dessus, la position de l'Afrique du Sud diffère de celle de la Convention de Malabo[158].

Nigeria

Bien que le Nigeria ne dispose encore d'aucune loi traitant explicitement la responsabilité des

intermédiaires, la Commission des communications du Nigeria a publié un ensemble de directives relatives à la prestation des services Internet incluant un mécanisme de notification et de retrait et des dispositions de décharge pour les fournisseurs de services Internet agissant comme intermédiaires de contenu[159]. Conformément au modèle de « notification et de retrait », les directives de la Commission exigent que les fournisseurs de services Internet déconnectent les inscrits ou retirent le contenu lorsqu'ils sont avertis que l'activité ou le contenu enfreint les directives ou d'autres lois applicables[160]. Il est important de noter qu'il n'existe actuellement aucune jurisprudence publiquement disponible indiquant si et comment les directives ont été appliquées. Néanmoins, on peut avancer que le Nigeria a utilisé une version de la responsabilité des intermédiaires en interdisant Twitter[161] en juin 2021, arguant que la plateforme avait servi à « organiser, coordonner et exécuter » du contenu illégal[162]. À la suite de l'interdiction de Twitter, le gouvernement fédéral a émis une directive selon laquelle les réseaux sociaux et les plateformes Over-the-Top (OTT) (un service permettant aux utilisateurs de partager du contenu pré-enregistré et diffusé en direct) opérant dans le pays doivent s'enregistrer auprès de la Commission des affaires corporatives et obtenir une licence de la Commission nationale de l'audiovisuel[163]. Ces événements suggèrent une préférence du Nigeria pour la responsabilité stricte vis-à-vis du contenu affectant des « questions d'intérêt national ».

Kenya

La stratégie du Kenya vis-à-vis de la responsabilité des intermédiaires diffère de celles de l'Afrique du Sud et du Nigeria. La loi 20 de 2019 du Kenya portant modification sur les droits d'auteur et le projet de loi de 2020 proposé pour la propriété intellectuelle[164] protègent les droits d'auteur de travaux tels que les programmes informatiques, le contenu audio et audiovisuel et les œuvres littéraires. Empruntant largement au Digital Millennium Copyright Act américain, le projet de loi propose quatre décharges : le « transport », la mise en cache, l'hébergement et la localisation des informations[165]. Les titulaires de droits d'auteur peuvent envoyer une demande de retrait à un prestataire de services, à la suite de laquelle une non-conformité risque d'entraîner une peine de prison ou une amende pour ce dernier. Il faut toutefois remarquer que ces dispositions concernent les droits d'auteur de travaux tels que « les programmes informatiques, le contenu audio et audiovisuel », etc. dans le cadre de la loi du Kenya sur la PI. C'est pourquoi, par opposition à l'Afrique du Sud et au Nigeria, les dispositions de demande de retrait ne peuvent pas s'appliquer largement aux intermédiaires.

Cependant, la loi du Kenya de 2018 sur la lutte contre la cybercriminalité et l'utilisation abusive de l'informatique criminalise la publication de fausses données ou de fake news, le cyberharcèlement, la distribution illicite de messages obscènes ou intimes, la fraude informatique, la pornographie infantile et le cybersquatting[166]. L'obligation imposée aux utilisateurs vise à garantir l'exactitude du contenu avant sa publication en ligne, une infraction pouvant entraîner de lourdes sanctions comme des amendes ou une peine de prison. Mais les militants des droits numériques ont indiqué que certaines de ses dispositions manquent de clarté au niveau de la définition. Par exemple, la loi criminalise la publication de « fausses informations » sans définir clairement ce que sont les « fake news ». Après la sortie de la loi, du fait de divers problèmes, notamment l'ambigüité de ce qui constitue une infraction, la Bloggers Association of Kenya a déposé une requête la contestant et faisant valoir qu'elle est inconstitutionnelle, car limitant les droits de liberté d'expression et d'accès à l'information des utilisateurs[167].

Sénégal

Présentement, le Sénégal limite la responsabilité des intermédiaires et ne les soumet à aucune obligation spécifique de surveiller le contenu[168]. Selon la loi du Sénégal sur les transactions électroniques, les intermédiaires ne peuvent être tenus responsables pour avoir stocké du contenu dont ils ignoraient la nature illicite[169]. Néanmoins, le Sénégal exige que lorsque le contenu stocké sur des plateformes intermédiaires consiste en « des crimes contre l'humanité, une incitation à la haine raciale et de la pornographie infantile », les intermédiaires doivent en avertir les autorités[170]. La loi du Sénégal sur les transactions électroniques exige également des intermédiaires qu'ils appliquent un système de notification et de retrait en plus de s'assurer que des mécanismes sont en place pour retirer le contenu illégal ou en empêcher l'accès[171]. Comme susmentionné, il existe une disparité entre la décharge des intermédiaires par le Sénégal conformément à sa législation nationale et les règles plus strictes de responsabilité des intermédiaires stipulées par la Convention de Malabo, ratifiée par le Sénégal[172]. Par exemple, là où le Sénégal exclut la responsabilité des intermédiaires stockant sans le savoir du contenu illicite, la Convention de Malabo prévoit qu'ils soient poursuivis. Et bien que la position du Sénégal manque de clarté quant à la responsabilité des intermédiaires du fait de cette divergence, sa ratification de la Convention de Malabo l'oblige légalement à revoir sa législation nationale pour refléter les lois sur la responsabilité des intermédiaires.

3.5 Droits de douane sur les transmissions électroniques

Alors que le commerce numérique s'accroît, les gouvernements recherchent des méthodes viables de collecte de revenus n'entravant pas la croissance économique. À cet égard, les pays (plus particulièrement développés et en développement) sont divisés quant à l'imposition ou non de droits de douane sur les transmissions électroniques. Si plusieurs accords commerciaux, par exemple l'ALE Singapour–Australie, l'accord de partenariat économique Japon–Suisse et l'ALE Nouvelle-Zélande–Taïwan ont inclus des dispositions sur l'interdiction des droits de douane, la plupart des pays africains de l'OMC ont adopté une position ferme en faveur de l'imposition de droits de douane sur les transmissions électroniques.

En 1998, les membres de l'OMC ont convenu d'un moratoire de deux ans (moratoire de l'OMC) interdisant aux pays d'imposer des droits de douane sur les transmissions électroniques, afin d'encourager ce nouvel aspect du commerce mondial. Bien que les membres aient respecté le moratoire de l'OMC, c'est un sujet de controverse pour plusieurs raisons. Les membres sont en désaccord sur la définition des « transmissions électroniques », dont la portée reste donc floue. Une étude du secrétariat de l'OMC menée en 2016 a strictement défini les transmissions électroniques comme « biens numérisables » incluant « les films cinématographies, les livres, les journaux et publications périodiques imprimés, les jeux électroniques (vidéo), les logiciels, les disques de musique, les bandes et les autres supports pour l'enregistrement du son ou pour enregistrements analogues, et les autres supports enregistrés »[173]. Cette interprétation des transmissions électroniques, qui couvre le contenu transmis électroniquement, est une définition partagée par certains membres de l'OMC (pour la plupart des pays développés)[174]. Mais d'autres

membres contestent cette définition, car ils considèrent les transmissions électroniques comme plus vastes et incluant le support de transmission[175] ou « tout objet physique capable de stocker les codes numériques composant un produit numérique via toute méthode déjà connue ou développée, reproduite ou communiquée ultérieurement, directement ou indirectement, y compris un support optique, une disquette et une bande magnétique »[176].

Les membres de l'OMC sont également en désaccord sur le fait d'interdire de façon permanente ou non les droits de douane sur les transmissions électroniques. Les propositions favorables au moratoire ont cité des bénéfices tels que l'amélioration de l'accès des consommateurs aux nouveaux produits et services grâce à la suppression de lourds droits de douane[177]. Mais certaines questions restent en suspens quant à la répartition égale entre les pays des gains de telles modalités. Les pays en développement s'opposent à l'adoption permanente de l'interdiction, considérant qu'elle « accorde aux pays avancés numériquement un accès en franchise [à leurs] marchés »[178]. Par exemple, le Groupe africain de l'OMC estime que l'interdiction des droits de douane sur les transmissions électroniques nuirait aux pays en développement et provoquerait des pertes de revenus considérables[179]. Appuyant cet argument, un rapport de 2019 de la CNUCED a révélé que, pour les pays d'Afrique subsaharienne en particulier, une perte potentielle de recettes douanières serait probablement deux fois supérieure à celle des pays développés de l'OMC si le moratoire était définitivement adopté[180]. Cependant, il a été avancé que par rapport aux recettes gouvernementales totales, cette part est très faible et concentrée uniquement entre quelques-uns des plus grands pays en développement[181].

Afrique du Sud

L'Afrique du Sud n'a pas encore de législation sur les droits de douane appliqués aux transmissions électroniques. Néanmoins, le pays a exprimé ses préoccupations quant à la portée du moratoire de l'OMC et à la perte consécutive de recettes douanières, ainsi qu'au possible impact négatif du moratoire sur la croissance économique induite par le numérique dans les pays en développement[182]. Cette inquiétude est liée à la fracture numérique entre les pays développés et en développement, en raison de laquelle les pays développés profitent davantage du moratoire[183].

Nigeria

Tout comme l'Afrique du Sud, le Nigeria n'a pas de lois directes sur l'imposition de droits de douane appliqués aux transmissions électroniques.

Kenya

Le Kenya n'a pas non plus de lois directes sur l'imposition de droits de douane appliqués aux transmissions électroniques. Toutefois, il fait aussi partie du Groupe africain de l'OMC opposé à l'adoption permanente du moratoire. Compte tenu de la position du Kenya, il reste à savoir si le pays maintiendra cette position dans le contexte du projet d'ALE avec les États-Unis. Bien qu'il ne soit pas encore conclu, les experts soutiennent que les États-Unis chercheront à interdire ces droits afin de ne pas désavantager les entreprises américaines, avec des répercussions négatives pour les start-ups locales beaucoup plus petites[184].

Sénégal

Le Sénégal, tout comme le Groupe africain de l'OMC, s'est fermement opposé à l'adoption permanente du moratoire de l'OMC interdisant l'imposition de droits de douane sur les transmissions électroniques. Selon cette position, l'interdiction des droits de douane sur les transmissions électroniques nuirait aux pays en développement et provoquerait une perte de revenus considérable[185].

4. Conclusion

Cette étude met en lumière les divergences existant au niveau de la manière dont quatre membres de la ZLECAf réglementent cinq enjeux de politiques spécifiques relatifs au commerce numérique. Cette étude montre que dans certains domaines spécifiques des politiques (par exemple la réglementation des signatures électroniques et la responsabilité des intermédiaires), les quatre pays adoptent des stratégies très différentes, bien qu'elles se composent d'éléments similaires. Par exemple, si les quatre pays reconnaissent la validité des signatures électroniques, ils divergent quant aux types de signatures électroniques reconnus juridiquement et aux circonstances dans lesquelles ces signatures sont considérées valables. Sur le plan de la responsabilité des intermédiaires, l'Afrique du Sud, le Nigeria et le Sénégal disposent tous de lois déchargeant les intermédiaires, mais se basent sur différents critères.

L'étude souligne également que dans certains domaines de politiques (comme la divulgation obligatoire du code source), même si les quatre pays ont un intérêt commun, il demeure des divergences vis-à-vis du degré de réglementation, d'implémentation et d'application des règles. Plus précisément, le Nigeria est le seul des quatre pays à exiger des entreprises multinationales qu'elles divulguent leur code source avant de déployer des logiciels sur son sol. Les trois autres pays ont adopté des règles demandant ou encourageant le partage du code source pour l'usage public. Il est aussi important de noter que dans certains domaines de politiques (par exemple les flux de données transfrontaliers), il existe des divergences entre les législations nationales et régionales. Par exemple, tandis que certains instruments tels que l'Acte additionnel de la CEDEAO empruntent majoritairement au RGPD de l'UE, le Nigeria (qui est membre de la CEDEAO) impose encore des règles strictes de localisation des données.

Le principal objectif des négociations de Phase II de la ZLECAf étant l'harmonisation de réglementations spécifiques pour améliorer le commerce intra-africain et encourager le commerce international avec la région, il est essentiel que les membres de la ZLECAf examinent les différences entre leurs politiques et stratégies de réglementation nationales. Une vision de ces divergences permettra aux membres de la ZLECAf de peser leurs coûts et de déterminer si une harmonisation est nécessaire et efficace pour les enjeux clés. En outre, réfléchir à ces questions indiquera où il existe un potentiel d'interopérabilité, grâce à quoi les membres pourront considérer si la ZLECAf est la plateforme adéquate pour l'harmonisation ou l'interopérabilité.

Notes

Ceci exclut le Sénégal, dont les lois actuelles ont pour modèle la directive de l'UE sur la protection des données et les lois ultérieures empruntent au RGPD.

2 Aux fins de ce rapport, le commerce numérique est défini comme des transactions numériques comprenant l'échange de biens et de services fournis numériquement ou physiquement et impliquant consommateurs, entreprises et gouvernements. Il est étroitement lié au commerce électronique défini par l'OMC comme la production, la distribution, le marketing, la vente ou la fourniture de biens et de services par voie électronique lors de transactions impliquant des entreprises, des ménages, des individus, des gouvernements et d'autres organisations publiques ou privées.

3 Pour un examen approfondi de la définition du commerce numérique, voir Emily Jones et al. (2021), *The UK and Digital Trade: Which Way Forward?* Blavatnik School of Government. Consultable ici : https://www.bsg.ox.ac.uk/ research/publications/uk-and-digital-trade-which-way-forward.

4 Susan Aaronson et Patrick Leblond (2018), Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO, *Journal of International Economic Law 1.*

5 Bai Gao et Yi Ru (2021), Industrial Policy and Competitive Advantage: A Comparative Study of the Cloud Computing Industry in Hangzhou and Shenzhen, dans Baark, Hofman et Qian (éd.) *Innovation and China's Global Emergence,* National University of Singapore Press, 232. Consultable ici : epress.nus.sg/ innovationandchina/InnovationandChinasGlobalEmergence.pdf#page=242.

6 Faith Tigere (2021), *The WTO and Africa: The State of Play and Key Priorities Going Forward,* SAIIA, briefing de politique, 243. Consultable ici : https://saiia.org.za/research/the-wto-and-africa-the-state-of-play-and-key- priorities-going-forward.

7 OCDE (2021), *Members of the OECD/G20 Inclusive Framework on BEPS*. Consultable ici : https://www.oecd.org/ tax/beps/inclusive-framework-on-beps-composition.pdf.

8 Jonathan Kamoga, 13 Countries Urged to Ratify Trade Deal, *The EastAfrican* (16 novembre 2021). Consultable ici : https://www.theeastafrican.co.ke/tea/business/13-countries-urged-to-ratify-trade-deal-3620340.

9 Mira Burri et Rodrigo Polanco (2020), Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset, *Journal of International Economic Law*, Volume 23, 187, 193.

10 Burri et Polanco (n 9).

Lillyana Daza Jaller et Martin Molinuevo (2020), *Digital Trade in MENA: Regulatory Readiness Assessment,* document de travail de recherches politiques n°6, Banque mondiale. Consultable ici : https://openknowledge.worldbank.org/ bitstream/handle/10986/33521/Digital-Trade-in-MENA-Regulatory-Readiness-Assessment.pdf.

Jaller et Molinuevo (n 11) 8.

Taku Nemoto et Javier López González (2021), Digital Trade Inventory: Rules, Standards and Principles, OCDE. Consultable ici : https://www.oecd-ilibrary.org/docserver/9a9821e0-en.pdf.

14 Minyan Wang (2006), *A Review of Electronic Signatures Regulations: Do They Facilitate or Impede International Electronic Commerce?* Centre for Commercial Law Studies, 548, 548.

15 Les signatures électroniques étant définies comme « des symboles ou autres données au format numérique apposés à un document transmis par voie électronique pour confirmer l'intention de l'expéditeur de signer le document » et les signatures numériques comme « un type de signature électronique chiffrant des documents avec des codes numériques particulièrement difficiles à dupliquer » (définitions de l'Oxford Dictionary).

16 Wang (n 14) 548.

17 Ibid.

18 Wang (n 14) 549.

19 Ibid.

20 Wang (n 14) 549; Emily Jones et al. (2021), *The UK and Digital Trade: Which Way Forward?* Document de travail de la BSG, série 41. Consultable ici : https://www.bsg.ox.ac.uk/sites/default/files/2021-02/BSG-WP-2021-038_0.pdf.

Jones et al. (n 20) 40.

Ibid.

Wang (n 14) 549. ; Jones et al. (n 20) 41.

24 CNUCED (2021), E-Transactions Legislation Worldwide (UNCTAD Cyberlaw Tracker). Consultable ici : https://unctad.org/page/e-transactions-legislation-worldwide.

25 Forum économique mondial (2017). *Making Deals in Cyberspace: What's the Problem?*

26 Loi sur les communications et transactions électroniques, 2002.

27 Karishma Banga, Jamie Macleod et Max Mendez-Parra (2021), *Digital Trade Provisions in the AfCFTA: What Can We Learn from South–South Trade Agreements?* 28.

28 Loi sur les communications et transactions électroniques, 2002.

29 Acte additionnel de 2010 de la CEDEAO relatif à la protection des données à caractère personnel, 2010 s 34 ; Loi du Nigeria sur la cybercriminalité (interdiction, prévention, etc.), 2015 s 17(1)(a).

30 Loi sur la preuve du Nigeria, 2011 s 93(3).

Une signature répondant à toutes les obligations suivantes : (i) elle est liée uniquement au signataire ; (ii) elle permet
d'identifier le signataire ; (iii) elle a été créée via des méthodes dont le signataire peut garder le contrôle exclusif ; et (iv) elle est liée aux données concernées de telle sorte que toute modification ultérieure des données
soit détectable.

Loi du Kenya portant modification du droit

commercial, 2020. Ibid.

34 William Maema et Imelda Anika (2020), What It Means to Use Electronic Signatures, *Insights*, DLA Piper Africa. Consultable ici : https://www.dlapiperafrica.com/en/kenya/insights/2020/what-it-means-to-use-electronic-

signatures.html.

35 Loi n°2008-08 sur les transactions électroniques, 2008.

36 Ceci inclut la société d'économie mixte GAINDE 2000, qui gère le Guichet unique du Sénégal et a introduit un environnement de commerce sans support papier dans ce pays.

37 CEE-ONU (2016), A Road Towards Paperless Trade: Senegal's Experience, *Trade Facilitation Implementation Guide: Case Stories*, 1. Consultable ici : https://tfig.unece.org/cases/Senegal.pdf.

38 Alfred Filani (2020), E-Commerce and Enforcement of Consumer Rights in Nigeria: Issues, Prospects and Challenges, *Journal of Law and Judicial System*, Volume 3, Issue 1, 1.

39 Tunde Ibidapo-Obe (2011), *Online Consumer Protection in E-Commerce Transactions in Nigeria: An Analysis*, Université du Sussex. Consultable ici : https://www.researchgate.net/publication/314459028_Online_Consumer_ Protection_in_E-Commerce_Transactions_in_Nigeria_An_Analysis.

40 Jones et al. (n 20) 41.

41 Karishma Banga et al. (2021) *E-Commerce in Preferential Trade Agreements: Implications for African Firms and the AfCFTA*, ODI, 15. Consultable ici : https://cdn.odi.org/media/documents/e-commerce_in_preferential_ trade_agreements_report.pdf ; Despoina Mantzari et Ioannis Lianos, *The Global Governance of Online Consumer Protection and E-Commerce: Building Trust*, Forum économique mondial (2019) 19. Consultable ici : www3.weforum.org/docs/WEF_consumer_protection.pdf ; Jones et al. (n 20).

42 Loly Gaitan et Julien Grollier (2020), *Electronic Commerce in Trade Agreements: Experiences of Small Developing Countries*, CUTS International, 26. Consultable ici : www.cuts-geneva.org/pdf/eAfCFTA-Study- E-Commerce_Provisions_in_RTAs.pdf.

43 Gaitan et Grollier (n 42) 27.

44 Transactions électroniques et commerce électronique : loi type de la Communauté de développement de l'Afrique australe (CDAA), 2013 pt IV.

45 Banga et al. (n 41).

46 Loi sur les communications et transactions électroniques, 2002.

47 Ibid.

48 Loi sur les communications et transactions électroniques, 2002.

49 Loi fédérale du Nigeria sur la concurrence et la protection des consommateurs, 2018.

50 Ifeoluwa Adeyemo, Nigeria Consumer Council Sets New Guidelines to Protect E-Commerce Consumers, *Nigeria Premium Times* (15 mars 2018). Consultable ici : https://www.premiumtimesng.com/business/business- news/261961-nigeria-consumer-council-sets-new-guidelines-to-protect-e-commerce-consumers.html.

51 Adeyemo (n 50).

52 Loi kenyane de protection du consommateur, 2012.

[53] Ibid. s 2.

[54] Ibid. s 31, 32, 33.

[55] Décret relatif au commerce électronique pris pour l'application de la loi n°2008 sur les transactions électroniques, 2008 s 10.

[56] Ibid. s 15.

[57] Ibid.

[58] Taku Nemoto et Javier López González (2021), *Digital Trade Inventory: Rules, Standards and Principles*, OCDE, 8. Consultable ici : https://www.oecd-ilibrary.org/docserver/9a9821e0-en.pdf.

[59] Anupam Chander et Martina Ferracane (2019), Regulating Cross-Border Data Flows – Domestic Good Practices, in *Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic Interdependence*, Forum économique mondial, 7. Consultable ici : https://www3.weforum.org/docs/WEF_ Trade_Policy_Data_Flows_Report.pdf.

[60] Francesca Casalini et Javier López González (2019), *Trade and Cross-Border Data Flows*, documents de travail de l'OCDE sur la politique commerciale, n°220, OCDE, 5. Consultable ici : https://www.sipotra.it/old/wp-content/uploads/2019/01/Trade-and- Cross-Border-Data-Flows.pdf.

[61] Banque mondiale (2021), *World Development Report: Data for Better Lives*. Consultable ici : https://www.worldbank.org/ en/publication/wdr2021.

[62] Banque mondiale (n 61) 238–241.

[63] Shaffer Gregory (2002), *Managing U.S-EU Trade Relations through Mutual Recognition and Safe Harbor Agreements: "New" and "Global" Approaches to Transatlantic Economic Governance?* Documents de travail de l'Institut universitaire européen, Robert Schuman Centre for Advanced Studies, 22–23.

[64] Reyes Carla (2011), WTO-Compliant Protection of Fundamental Rights: Lessons From the EU Privacy Directive, *Melbourne Journal of International Law*, Volume 12, 6. Consultable ici : https://law.unimelb.edu.au/ data/assets/ pdf_file/0010/1686934/Reyes.pdf ; Svetlana Yakovleva et Kristina Irion (2020), Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows With External Trade, *International Data Privacy Law*, Volume 10, Issue 3, Oxford University Press, 6.

[65] Reyes Carla (n 64) 6.

[66] Alexander Beyleveld (2021), *Data Localisation in Kenya, Nigeria and South Africa: Regulatory Frameworks, Economic Implications and Foreign Direct Investment*, briefing de politique 07, Mandela Institute. Consultable ici : https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/ research-entities/mandela-institute/documents/research-publications/800553%20PB7%20Data%20 localisation%20and%20FDI%20in%20Kenya%2001A.pdf

[67] Wu T (2006), The World Trade Law of Censorship and Internet Filtering, *Chicago Journal of International Law*, Issue no. 7, 281.

[68] Martina Ferracane (2018), *South Africa and Data Flows*, document de travail de GEGAfrica, avril 2018. Consultable ici : https://www.gegafrica.org/item/651-south-africa-and-data-flows-how-to-fully-exploit-the-potential-of-the- digital-economy.

[69] Shanelle van der Berg (2021), *Data Protection in South Africa: The Potential Impact of Data Localisation on South Africa's Project of Sustainable Development*, Mandela Institute, briefing de politique, série 6.

[70] Pathways for Prosperity Commission (2019), Digital Diplomacy: Technology Governance for Developing Countries, Université d'Oxford, 35. Consultable ici : https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-10/ Digital-Diplomacy.pdf.

[71] Christopher Foster et Shamel Azmeh (2020), Latecomer Economies and National Digital Policy: An Industrial Policy Perspective, *Journal of Development Studies* 56 (2), 1247, 1259.

[72] Institut de la finance internationale (2020), *Data Localisation: Costs, Tradeoffs, and Impacts Across the Economy*. Consultable ici : https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.

[73] Institut de la finance internationale (n 72) 5.

[74] Union africaine (2020), *The Digital Transformation Strategy for Africa (2020–2030).*

[75] Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, 2014.

[76] Union africaine (2020), *Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel - Liste de statuts.*

[77] Koliw Majam et Janny Montinat (2021), *Privacy and Personal Data Protection in Africa: Advocacy Toolkit*, Coalition de la Déclaration africaine des droits et libertés de l'Internet, 37. Consultable ici : https://www.apc.org/en/pubs/privacy- and-personal-data-protection-africa-advocacy-toolkit.

[78] Majam et Montinat (n 77) 36.

[79] Sylla, A, Ford-Cox, A (2019), *Overview of data protection laws in Africa*. Lexology. Consultable ici : https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2

[80] Moritz Hennemann et Patricia Boshe (à paraître), African Data Protection Laws, Global Privacy Law Review, 35. Consultable ici : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3947664

[81] Patricia Boshe (n 80) 35.

[82] CNUCED (2021), *Digital Economy Report 2021, xv*. Consultable ici : https://unctad.org/webflyer/digital-economy- report-2021.

[83] Michael Pisa et Ugonma Nwako (2021), *Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development: Roundtable Summary*, Centre for Global Development, 2. Consultable ici : https://www.cgdev.org/sites/default/files/are-current-models-data-protection-fit-purpose- understanding-consequences-economic.pdf.

[84] La plupart des dispositions de fond sont entrées en vigueur le 1er juillet 2020, bien que certaines règles n'aient démarré que le 30 juin 2021.

[85] Bien qu'elle ressemble beaucoup au RGPD de l'UE, la loi POPI de l'Afrique du Sud ne concerne que les parties responsables domiciliées en Afrique du Sud ou utilisant des moyens automatisés ou non automatisés en Afrique du Sud.

[86] Loi sur les communications électroniques : version préliminaire de la politique nationale sur les données et le cloud 2021, Global Data Alliance, commentaires adressés à la République d'Afrique du Sud pour le projet de politique sur les données et le cloud (avril 2021). Consultable ici : https://www.globaldataalliance.org/downloads/05122021gdasafrdatacloud.pdf.

[87] Loi sur les communications électroniques : version préliminaire de la politique nationale sur les données et le cloud.

[88] van der Berg (n 69) 3.

[89] Règlement nigérian sur la protection des données, 2019.

[90] Directives pour le développement de contenu nigérian dans les technologies de l'information et de la communication (TIC), 2019 s 2.11.

[91] Ibid. s 2.10.

[92] Règlement nigérian sur la protection des données, 2019.

[93] Kenneth Erikume et Wunmi Adetokunbo-Ajayi (2020), The NDPR and the Data Protection Bill 2020, pwc. Consultable ici : https://www.pwc.com/ng/en/publications/data-protection-bill-2020.html.

[94] Politique du Nigeria sur le cloud computing, 2019.

[95] Directives pour le développement de contenu nigérian dans les technologies de l'information et de la communication (TIC).

[96] Banque centrale du Nigeria (2011). Directive sur les services d'acceptation des cartes dans les points de vente (PDV). Section 4.4.8.

[97] Protocole de la ZLECAf sur le commerce des services.

[98] Loi du Kenya sur la protection des données, 2019 ; Règlement (général) sur la protection des données du Kenya, 2021.

[99] Définition de « nécessaire » : (i) pour l'exécution d'un contrat entre le sujet des données et le contrôleur des données ou le processeur des données, ou l'implémentation de mesures précontractuelles prises à la demande du sujet des données ; (ii) pour la conclusion ou l'exécution d'un contrat conclu dans l'intérêt du sujet des données entre le contrôleur et une autre personne ; (iii) pour toute question d'intérêt public ; (iv) pour l'établissement, l'exercice ou la défense d'une demande légale ; (v) pour la protection d'intérêts fondamentaux du sujet des données ou d'autres personnes, lorsque le sujet des données est physiquement ou légalement incapable de donner son consentement ; ou (vi) à des fins d'intérêts légitimes impérieux poursuivis par le contrôleur ou le processeur des données et n'étant pas supplantés par les intérêts, les droits et les libertés des sujets des données.

[100] Loi du Kenya sur la protection des données, 2019.

[101] Loi du Kenya sur la protection des données, 2019.

[100] Règlement (général) sur la protection des données du Kenya, 2021.

[103] Voir l'Accord de partenariat économique entre le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord d'une part et la République du Kenya, un membre de la Communauté d'Afrique de l'Est, d'autre part, Protocole 2, Articles 10 et 13.

[104] Bureau du représentant américain au Commerce (2020), United States-Kenya Negotiations: Summary of Specific Negotiating Objectives, 7. Consultable ici : https://ustr.gov/sites/default/files/Summary_of_U.S.-Kenya_ Negotiating_Objectives.pdf.

[105] Loi portant sur la protection des données à caractère personnel, 2008.

[106] Ibid.

[107] Loi sur la protection des données personnelles, 2019 s 8.

[108] Loi sur la protection des données personnelles, 2019.

[109] Loi portant sur la protection des données à caractère personnel, 2008 ; Loi sur la protection des

données personnelles, 2019.

110 Compte tenu des lacunes actuelles de son système, le Sénégal n'a pas obtenu de décision d'adéquation de l'UE.

Conseil de l'Europe (2021), Convention 108 et protocoles. Consultable ici : https://www.coe.int/en/web/data- protection/convention108-and-protocol.

OMC (2017), *Some Preliminary Implications of WTO Source Code Proposal*, briefings du Third World Network, 4. Consultable ici : https://twn.my/MC11/briefings/BP4.pdf.

Muhammad Irfan (2019), *Data Flows, Data Localisation, Source Code: Issues, Regulations and Trade Agreements*, CUTS International, 16. Consultable ici : www.cuts-geneva.org/pdf/WTOSSEA2018-Study-Data_Flows_ Localisation_Source_Code.pdf.

114 Irfan (n 113) 17.

115 CNUCED (2014) *Studies in Technology Transfer: Selected Cases from Argentina, China, South Africa and Taiwan Province of China*, 2. Consultable ici : https://unctad.org/system/files/official-document/dtlstict2013d7_en.pdf.

116 L'accord ADPIC définit les normes minimales de divers éléments de la PI, y compris les brevets, les marques déposées, les droits d'auteur et les secrets industriels.

117 OMC (1994), Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce, 1994 s 66.2. Consultable ici : https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm.

118 OMC (2019), Joint Statement on Electronic Commerce: Communication from Singapore. INF/ECOM/25. Consultable ici : https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/25.pdf&Open=True.

119 Irfan (n 113) 17.

120 Jones et al. (n 3).

Accord Canada–États-Unis–Mexique, 2018.

Accord de partenariat économique global Japon–Royaume-Uni, 2020.

Irfan (n 113) 16.

124 Valente, MG (2020), *Digital Technologies and Copyright: International Trends and Implications for Developing Countries*, série de documents de Digital Pathways at Oxford, n°1. Consultable ici : https://pathwayscommission.bsg.ox.ac. uk/Mariana-Valente-digital-technologies-and-copyright.

125 Lee Raine et Janna Anderson (2017), *Code-Dependent: Pros and Cons of the Algorithm Age*, Pew Research Center. Consultable ici : https://www.pewresearch.org/internet/2017/02/08/code-dependent-pros-and-cons-of- the-algorithm-age.

126 Sandra Wachter, Brent Mittelstadt et Chris Russell (2018), Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, *Harvard Journal of Law and Technology*, Volume 31, 841.

127 Valente (n 124).

128 L'ARIPO a été établie lors de l'accord de Lusaka de 1976 pour favoriser la coopération entre les États membres à l'égard de la propriété industrielle et progresser sur le plan technologique afin de soutenir le développement économique et industriel. Actions employées (entre autres) : (i) encourager l'harmonisation et le développement de lois sur la propriété industrielle adaptées aux besoins des membres ; (ii) établir les

services ou organes communs nécessaires à la coordination ; et (iii) encourager l'échange d'idées et d'expérience, la recherche et les études concernant les questions de propriété industrielle.

129 L'OAPI a été créée en mars 1977 via l'Accord de Bangui pour encourager les États membres à coopérer, construire des réseaux et partager des ressources communes en matière de propriété intellectuelle. L'Accord de Bangui sert de loi nationale pour chacun des 17 États, principalement situés en Afrique francophone.

130 Politique sur l'utilisation de logiciels libres et gratuits par le gouvernement sud-africain, 2006.

Ibid.

Loi sur les droits de propriété intellectuelle émanant du financement public en matière de recherche et de développement : réglementations, 2008 ; Nazeem Mustapha et Gerard Ralphs (2021), Effectiveness of Technology Transfer in Public Research Institutions in South Africa: A Critical Review of National Indicators and Implications for Future Measurement, *African Journal of Science, Technology, Innovation and Development*, 1.

133 Le Bureau national de gestion de la propriété intellectuelle, établi par la loi sur les droits de propriété intellectuelle émanant du financement public en matière de recherche et de développement de 2008, et faisant partie du ministère de la Science et de la Technologie, est responsable d'appliquer ces dispositions.

134 Ministère de la Science et de la Technologie, République d'Afrique du Sud (2019), *White Paper on Science, Technology and Innovation 2019*. Consultable ici : https://www.dst.gov.za/images/2019/White_paper_web_copyv1.pdf.

135 Directives pour le développement de contenu nigérian dans les technologies de l'information et de la communication (TIC).

136 Ibid.

137 Politique nationale du Kenya sur les TIC, 2019.

138 Ibid.

139 Mawaki Chango et Sadio Insa (2020), *Évaluation du développement de l'Internet au Sénégal : utilisation des indicateurs ROAM-X de l'universalité de l'Internet de l'UNESCO*, UNESCO, 68. Consultable ici : https://unesdoc. unesco.org/ark:/48223/pf0000374740.

140 Les plateformes Internet sont considérées comme des intermédiaires lorsque leurs services incluent la réception, le stockage et la transmission de contenus générés par les utilisateurs, et qu'elles ne publient pas le contenu elles-mêmes (Facebook, YouTube et Twitter appartiennent à cette catégorie).

141 Ashley Johnson et Daniel Castro (2021), *How Other Countries Have Dealt with Intermediary Liability*, Information Technology & Innovation Foundation, 1. Consultable ici : https://itif.org/sites/default/files/2021- section-230-report-4.pdf.

142 Broadcasting Services Act de l'Australie, 1992 ; Loi indienne sur les technologies de l'information, 2000 ; Loi japonaise sur la limitation de la responsabilité des fournisseurs, 2001.

143 Johnson et Castro (n 141) 2.

144 Johnson et Castro (n 141) 4.

145 Au moment de la rédaction, les États-Unis envisageaient de réviser la section 230 sur la responsabilité des intermédiaires.

146 Communications Decency Act – Title V of the Telecommunications Act, États-Unis, 1996 ; Digital

Millennium Copyright Act, États-Unis, 1998 ; Johnson et Castro (n 141) 7.

147 Ashley Johnson et Daniel Castro (2021), *Fact Checking the Critiques of Section 230: What Are the Real Problems?* Information Technology & Innovation Foundation, 1. Consultable ici : https://itif.org/sites/default/files/2021-230- report-3.pdf.

148 Johnson et Castro (n 141) 7 ; Johnson et Castro (n 147).

149 Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel.

150 Global Network Initiative (2020), Trends in Content Regulation in Africa and Beyond, Report from the GNI Session at FIFAfrica. Consultable ici : https://medium.com/global-network-initiative-collection/trends-in-content- regulation-in-africa-and-beyond-report-from-the-gni-session-at-fifafrica-6c6a6e757f7e.

151 Jones et al. (n 3).

152 Loi sur les communications et transactions électroniques, 2002, ch XI.

153 Ibid.

154 Ibid.

155 Ibid.

156 Nicolo Zingales (2020), Intermediary Liability in Africa: Looking Back, Moving Forward?, dans Giancarlo Frosio (éd.), *Oxford Handbook of Online Intermediary Liability*. Consultable ici : https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138-e-11.

157 Alex Comninos (2012), *Intermediary Liability in South Africa*, Association for Progressive Communications, 5. Consultable ici : https://www.apc.org/sites/default/files/Intermediary_Liability_in_South_Africa-Comninos_ 06.12.12.pdf.

158 Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, 9 ; Zingales (n 156).

159 Directives relatives à la prestation des services Internet, 2008 ; Kasim Sodangi (2021), What Nigeria Needs to Ask from Twitter, Techcabal (27 juillet 2021). Consultable ici : https://techcabal.com/2021/07/27/what-nigeria-needs-to-ask- from-twitter.

160 Directives relatives à la prestation des services Internet.

161 Twitter sert d'intermédiaire.

162 Tage Kene-Okafor (2021), Twitter Ban in Nigeria to be Lifted if Platform Sets up a Local Office and Pays Taxes, President Says, TechCrunch (1er octobre 2021). Consultable ici : https://techcrunch.com/2021/10/01/twitter-ban-in- nigeria-to-be-lifted-if-platform-sets-up-a-local-office-and-pay-taxes-president-says.

163 Nan (2021), Why Twitter, other platforms must register to operate, *The Guardian.* (11 juin 2021). Consultable ici : https://guardian.ng/news/why-twitter-other-platforms-must-register-to-operate-fg.

164 Bien qu'il n'ait pas encore été promulgué, le projet de loi de 2020 sur la propriété intellectuelle vise à simplifier les procédures de PI en (entre autres) réunissant dans une seule loi toute la législation applicable actuelle, par exemple la loi sur la propriété industrielle de 2001, la loi sur les marques déposées (révisée en 2012), la loi sur les droits d'auteur de 2001 et la loi anticontrefaçon de 2008.

165 Projet de loi du Kenya sur la propriété intellectuelle, 2020 s 238.

166 Loi du Kenya sur la lutte contre la cybercriminalité et l'utilisation abusive de l'informatique, 2018 ss 22–24, 27, 28, 37.

167 *The Bloggers Association of Kenya (BAKE) v Attorney General & 5 others* [2018], Recours 206 auprès de la Haute cour du Kenya.

168 L'article 3(2) de la loi sur les transactions électroniques définit les intermédiaires comme « des personnes dont l'activité consiste à fournir un accès public à des services via des technologies de communication et d'information ».

169 Loi n°2008-08 sur les transactions électroniques s 3(2).

170 Ibid.

171 Ibid.

172 Tomslin Samme-Nlar (2018), *Why it is Important for African States to Ratify the Malabo Convention*, blog, African Academic Network on Internet Policy (31 juillet 2018). Consultable ici : https://aanoip.org/why-it-is-important-for- african-states-to-ratify-the-malabo-convention.

173 OMC (2016), secrétariat de l'OMC, Conseil général – *Fiscal Implications of the Customs Moratorium on Electronic Transmissions: The Case of Digitisable Goods*, OMC, JOB/GC/114.

174 Délégation de l'Union européenne (2019), *Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce*. INF/ECOM/22 3. Consultable ici : https://trade. ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

175 OMC (2017), Délégation de l'Indonésie, *Statement by Indonesia: Facilitator's Consultation on Electronic Commerce, MC11 Declaration, and Other Relevant Plenary Sessions* (13 décembre 2017). Consultable ici : https://docs.wto. org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/68.pdf&Open=True ; Nicolas Kohler-Suzuki (2020), *New Evidence on the Impact of Customs Duties for Digitisable Products and Electronic Transmissions:*
The Cases of Egypt and Vietnam, Dalberg, 4. Consultable ici : https://www.researchgate.net/publication/346787138_ New_evidence_on_the_impact_of_customs_duties_for_digitizable_products_and_electronic_transmissions_ The_cases_of_Egypt_and_Vietnam.

176 Law Insider, définition d'un support de transmission. Consultable ici : https://www.lawinsider.com/dictionary/carrier-medium.

177 Délégation de l'Union européenne (n 174).

178 OMC (2018), Délégations d'Afrique du Sud et d'Inde, *Work Programme on Electronic Commerce – Moratorium on Customs Duties on Electronic Transmissions: Need for a Re-Think*, \WT/GC/W/747. Consultable ici : https://docs. wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W747.pdf&Open=True.

179 OMC (2017), Groupe africain, *The Work Programme on Electronic Commerce: Statement by the African Group*. Consultable ici : https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueId List=239609,239579,239541,239472,239464,239336,239275,239266,239269,239278&CurrentCatalogueIdIndex=0&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=False&HasSpanishRecord=False.

180 Rashmi Banga (2019), *Growing Trade in Electronic Transmissions: Implications for the South*, CNUCED. Consultable ici : https://unctad.org/system/files/official-document/ser-rp-2019d1_en.pdf.

181 Simon Evenett (2021), *Is the WTO Moratorium on Customs Duties on E-Commerce Depriving Developing Countries of Much Needed Revenue?* St. Gallen Endowment, 5. Consultable ici : https://currentthoughtsontrade. com/wp-content/uploads/2021/11/S.-Evenett_-WTO-Moratorium-12-Nov-2021_-finalised.pdf.

182 OMC (2020), Délégations d'Inde et d'Afrique du Sud, *Work Programme on Electronic Commerce –The E-commerce Moratorium: Scope and Impact, Communication from India and South Africa*, 10 mars 2020, https://commerce. gov.in/wp-content/uploads/2020/11/E-Commerce-Moratorium-Scope-and-Impact.pdf

183 OMC (2019), Délégations d'Inde et d'Afrique du Sud, *Work Programme on Electronic Commerce – The E-Commerce Moratorium and Implications for Developing Countries: Communication from India and South Africa*. Consultable ici : https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=254770, 254764,254708,254719,254575,254574,254577,254349,254248,254192&CurrentCatalogueIdIndex=2&FullTextHash=237161575&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True.

184 Centre for Intellectual Property and Information Technology Law (2021), *The Impact of the Proposed US-KE FTA on Kenya's Data and Digital Trade Policy*.

185 Groupe africain de l'OMC (n 179).