Union Africaine

Une société intégrée et prospère
et une Afrique paisible

Principes d'intégration de dispositions relatives aux données dans les protocoles sur le commerce numérique

SEPTEMBRE 2023

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

REMERCIEMENTS

Les lignes directrices en matière d'intégration des dispositions relatives aux données du Protocole sur le commerce numérique ont été préparées sous la direction générale de S.E. le Dr Amani Abou-Zeid, commissaire aux infrastructures et à l'énergie, de l'équipe de la commission de l'UA composée du Dr Kamugisha Kazaura, directeur du département des infrastructures et de l'énergie, de M. Moses Bayingana, responsable par intérim de la Division Société de l'information et de Mme Souhila Amazouz, responsable principale de la politique numérique (coordonnatrice du groupe de travail), ainsi que des contributions et apports précieux des membres du groupe de travail représentant les communautés économiques régionales, l'AUDA-NEPAD, les institutions spécialisées de l'UA, les organisations régionales et panafricaines, le Réseau africain des autorités de protection des données (NADPA) ainsi que des agences des Nations unies et des organisations internationales opérant en Afrique dans le domaine des données et du commerce numérique.

Le cadre a bénéficié du soutien financier de la GIZ et de l'appui technique de M. Paul Baker, PDG d'International Economic Consulting Ltd.

Des commentaires ont également été reçus à différentes étapes de la production de ce document de la part des experts africains des États membres de l'UA participant aux ateliers de validation virtuels.

Ces lignes directrices ont été approuvées par la 44e session ordinaire du conseil exécutif, tenue en février 2024, et sont conformes au cadre stratégique en matière des données de l'UA, approuvé par le sommet de l'UA en février 2022

.

ACRONYMES

4IR	Quatrième révolution industrielle
ADR	Mode alternatif de règlement des conflits
Accord ZLECAf	Accord sur la zone de libre-échange continentale africaine
IA	Intelligence artificielle
APEC	Coopération économique pour l'Asie-Pacifique
API	Interface de programmation d'application
ANASE	Association des nations de l'Asie du Sud-Est
UA	Union africaine
B2B	Commerce électronique entre entreprises
BATNA	Meilleure alternative à un accord négocié
CAGR	Taux de croissance annuel composé
CBPR	Règles de confidentialité transfrontalières
CCPA	Loi californienne sur la protection de la vie privée des consommateurs
CPTPP	Accord de partenariat transpacifique global et progressiste
DEA	Partenariat numérique
APEN	Accord de partenariat sur l'économie numérique
DFFT	Libre circulation des données en toute confiance
DMF	Cadre de gestion des données
DPA	Loi sur la protection des données
MRD	Mécanismes de règlement des différends
STN	Stratégie de transformation numérique
Commerce électronique	Commerce électronique
CEDEAO	Communauté économique des États de l'Afrique de l'Ouest
UE	Union européenne
ALE	Accord de libre-échange
G20	Groupe des vingt
GATS	Accord général sur le commerce des services
GBP	Livre sterling
PIB	Produit intérieur brut
RGPD	Règlement général sur la protection des données
GMV	Volume brut de marchandises
TIC	Technologies de l'information et de la communication
IFC	Société financière internationale
IdO	Internet des objets
FAI	Fournisseurs d'accès à Internet
JSI	Déclaration conjointe sur l'initiative
CCT	Clauses contractuelles types
OCDE	Organisation de coopération et de développement économiques
POPIA	Loi sur la protection des renseignements personnels

RCEP	Partenariat économique régional global
CER	Communautés économiques régionales
ACR	Accords commerciaux régionaux
SADC	Communauté de développement de l'Afrique australe
ODD	Objectifs de développement durable
TAPED	Accords commerciaux sur le commerce électronique et les données
ACC	Accord de commerce et de coopération
TiSA	Accord sur le commerce des services
TPP	Accord de partenariat transpacifique
R.-U.	Royaume-Uni
ONU	Nations unies
CNUCED	Conférence des Nations unies sur le commerce et le développement
UNDG	Groupe des Nations unies pour le développement
É.-U.	États-Unis
$ US	Dollar américain
ACEUM	Accord Canada-États-Unis-Mexique
FEM	Forum économique mondial
OMC	Organisation mondiale du commerce
ZOPA	Zone d'accord possible

1. INTRODUCTION

1.1. TENDANCES DU DÉVELOPPEMENT INTERNATIONAL DE L'ÉCONOMIE NUMÉRIQUE

La numérisation est devenue une source majeure de croissance socio-économique. L'économie numérique valait 11 500 milliards de dollars à l'échelle internationale, soit 15,5 % du PIB mondial en 2016, et a connu depuis 2000 une hausse deux fois et demie plus rapide que le PIB mondial (Huawei & Oxford Economics, 2017). Les progrès réalisés dans l'élargissement de la connectivité ont suscité d'énormes opportunités de développement socio-économique. Aujourd'hui, 95 % de la population de la planète a accès à un réseau haut débit mobile, 63 % de la population mondiale ayant utilisé Internet en 2021 (GSMA, 2022; ITU, 2021). Selon GSMA (2023), en 2023, les technologies et services mobiles ont généré 5 200 milliards de dollars de valeur économique ajoutée, soit 5 % du PIB. La connectivité numérique a également démontré son rôle de stimulation de la résilience sociétale durant la crise de la COVID-19. Elle a en effet permis aux gens de poursuivre leurs activités sociales et économiques habituelles lors des confinements internationaux de 2020-2021 (ICC, 2022)..

Le commerce numérique évolue également à un rythme impressionnant. En termes d'échange de marchandises par le commerce électronique, la CNUCED estime que les ventes mondiales du commerce électronique ont atteint 26 700 milliards de dollars en 2019, le commerce électronique B2B représentant quant à lui 82 % de l'ensemble du commerce électronique (UNCTAD, 2021). Il ne fait aucun doute que la pandémie due à la COVID-19 a fait évoluer les habitudes d'achat, des achats hors ligne aux achats en ligne (UNCTAD, 2021). Le commerce des services fournis par voie électronique a également augmenté au fil des ans, avec une progression d'environ 7 % par an entre 2005 et 2021. En 2021, les exportations de services fournis par voie électronique se sont élevées à 3 800 milliards de dollars, représentant quelque 63 % du commerce mondial des services selon CNUCED.

Les données sont intégrées à l'ensemble des technologies d'avant-garde qui stimulent l'économie numérique.[1] Les données servent non seulement d'apports pour la production de biens et de services, mais possèdent en même temps des caractéristiques uniques (cf. Box 1) qui leur ont permis de devenir un facteur de compétitivité pour l'entreprise (Hagiu & Wright, 2020). Comme l'ont noté Giddlings *et al*. (2021), « *la numérisation économique et financière permanente transforme les données individuelles en un apport essentiel et une source de valeur pour les entreprises intersectorielles, des grandes sociétés de tech aux laboratoires pharmaceutiques en passant par les fabricants et les prestataires de services financiers. Des données sur le comportement et les choix de l'être humain — nos « préférences », habitudes d'achat, activités sociales, données biométriques et choix financiers — sont actuellement créées, collectées, stockées et traitées à une échelle inégalée.* »

1 Les CCDI — chaîne de blocs (blockchain), cloud, données et intelligence artificielle — sont considérés comme l'alphabet du futur. Cf. (GovTech Singapore, 2018; CloudSufi, 2021)

Case 1. Les caractéristiques uniques des données

La valeur ajoutée des données provient du traitement, de la transmission, du stockage et de la combinaison des données. Les données sont immatérielles et non rivales, ce qui signifie que quantité de gens peuvent exploiter les mêmes données en même temps ou au fil du temps, sans les épuiser. Du même coup, l'accès aux données peut être limité par des moyens techniques ou légaux, ce qui entraîne des niveaux d'exclusion variés. Par exemple, les données recueillies par d'importantes plateformes internationales ne sont pas aisément disponibles pour un usage par autrui, ce qui confère aux propriétaires de ces plateformes une position de monopole pour tirer parti des données. De plus, il peut arriver fréquemment que les valeurs agrégées soient supérieures à la somme des valeurs individuelles, en particulier en combinaison avec des données autres et complémentaires.[...]

En outre, les données ont un caractère multidimensionnel. D'un point de vue économique, les données peuvent fournir à ceux qui les collectent et les contrôlent non seulement une valeur privée, mais aussi une valeur sociale pour l'économie tout entière. La valeur sociale ne peut pas être garantie par les marchés seuls. De surcroît, la répartition de revenus privés issus de données est extrêmement inégale. En conséquence, l'élaboration de politiques est nécessaire pour supporter les objectifs d'efficacité et d'équité. Toutefois, des dimensions non économiques doivent aussi être prises en compte. En effet, les données sont étroitement liées à la vie privée et à d'autres droits de la personne, ainsi qu'à des questions de sécurité nationale, tous devant être abordés. Du point de vue des avantages socio-économiques, les données peuvent servir de conditions fondamentales ou de catalyseurs permettant aux gouvernements de fournir des services publics plus efficaces et une bonne gestion environnementale ainsi que d'améliorer la transparence et la gouvernance des actions gouvernementales.

En raison de ces avantages, la nécessité de disposer de données ouvertes, de normes d'interopérabilité et d'initiatives de partage des données a été soulignée afin d'exploiter le potentiel des données pour stimuler le développement, assurer une meilleure répartition des avantages des données, favoriser la confiance grâce à des garanties qui protègent les personnes contre les effets néfastes de l'utilisation abusive des données, créer et maintenir un système de données national intégré qui permet le flux de données entre un large éventail d'utilisateurs de manière à faciliter l'utilisation et la réutilisation en toute sécurité des données.

Source : (UNCTAD, 2021; African Union, 2022)

1.2. LE POTENTIEL DE L'ÉCONOMIE NUMÉRIQUE DE L'AFRIQUE

L'économie numérique de l'Afrique est en passe de devenir une source de croissance énorme et solide. Le continent connaît une croissance substantielle de la téléphonie mobile, 61 % et 40 % de la population respectivement ayant désormais accès aux téléphones portables et à Internet. Le développement des services à haut débit est impressionnant, sous l'impulsion du haut débit mobile, auquel 42 % de la population a eu accès en 2022 (ITU, 2022). Selon un rapport conjoint d'IFC et de Google (2020), l'économie numérique africaine a le potentiel opportun pour ajouter 180 milliards de dollars au produit intérieur brut (PIB) de l'Afrique d'ici 2025. À l'heure actuelle, dix-neuf des vingt pays du monde où la croissance est la plus rapide sont en Afrique. Ce continent dispose en plus d'une main-d'œuvre de plus en plus urbanisée, la plus jeune du monde, et qui croît le plus rapidement (Google & IFC, 2020). On s'attend à ce que ces données démographiques – associées à une longévité et des niveaux de formation meilleurs, des investissements d'envergure dans les infrastructures TIC, une concurrence optimisée entre les fournisseurs d'accès à Internet (FAI) – boostent la demande et la capacité d'approvisionnement de biens et de services numériques, en contribuant à la croissance économique numérique du continent.

Bien que toujours confrontée à plusieurs défis infrastructurels et de gouvernance, l'économie numérique en Afrique est tirée par de jeunes entrepreneurs dynamiques spécialisés dans le numérique. Des start-ups sont en train de résoudre certains des problèmes les plus criants de l'Afrique. On y trouve l'accès aux soins de santé des populations isolées, les opportunités d'emploi pour les femmes et les possibilités d'envoi et de réception sécurisés d'argent. Nombreux sont les consommateurs africains à avoir vécu un saut dans l'inconnu en passant directement des espèces aux paiements mobiles sans n'avoir jamais détenu une carte en plastique – un récit admiré et reproduit par bien des pays du monde (Smart Africa Alliance, 2021). L'histoire à succès des moyens de paiement prioritairement mobiles de l'Afrique a renforcé la foi dans l'élaboration d'une solution africaine. Les nouveaux modèles d'entreprise en Afrique tirent désormais avantage des technologies de pointe — taillées sur mesure pour des approches axées sur les données, évolutives et panafricaines (Google & IFC, 2020).

Les marchés des données de l'Afrique sont en voie de doubler tous les cinq à six ans. On estime que la valeur des marchés des données en Afrique atteindra 3 milliards de dollars d'ici 2025, pour progresser de plus de 12 % entre 2019 et 2025 (Koigi, 2020). Le secteur a bénéficié d'investissements de 2,6 milliards de dollars en 2021 (Research and Markets, 2022). L'industrie africaine des centres de données fait l'objet d'un intérêt constant des principaux prestataires de services cloud comme AWS et Microsoft, sans oublier Huawei ces cinq dernières années (Koigi, 2020).

1.3. LE RÔLE CRUCIAL DES DONNÉES DANS LA TRANSITION AFRICAINE VERS L'ÉCONOMIE NUMÉRIQUE

Les données contribuent de plus en plus aux transformations numériques et technologiques en alimentant de nouveaux modèles d'entreprise. En fait, on décrit les données comme le nouveau « pétrole » (Rotella, 2012). En effet, si données et pétrole ont bien une valeur intrinsèque, tous deux doivent être « raffinés » ou transformés d'une autre manière pour déployer leur plein potentiel (World Bank, 2021). De nos jours, les données sont considérées comme un atout et une source possible de croissance et d'innovation. Le volume grandissant de données à caractère personnel et non personnel, industrielles et publiques, combinées aux technologies émergentes telles que l'Intelligence Artificielle (IA), l'Internet des objets (IdO) et le cloud computing, a considérablement impacté les modes de collecte, de stockage, de traitement et de transmission à travers la planète. L'importance des données pour les sociétés modernes exige une perspective de politique stratégique de haut niveau susceptible d'équilibrer des objectifs politiques multiples – de la libération du potentiel économique et social des données à l'atténuation des risques liés à la collecte et au traitement en masse des données à caractère personnel.

L'Afrique peut voir émerger prochainement des opportunités considérables de la transformation numérique. La production et l'utilisation sans cesse croissantes des données ont l'opportunité de soutenir le développement d'une économie durable et inclusive axée sur les données et d'une société conforme aux aspirations de l'Agenda 2063. Pour permettre aux pays d'exploiter l'énorme quantité de données à caractère personnel et non personnel, industrielles et publiques générées par leurs citoyens et les industries, ainsi que pour faciliter la circulation intersectorielle et transfrontalière des données, il est indispensable d'encourager l'instauration d'un espace de données commun et la création d'un environnement politique favorable et porteur pour dynamiser l'innovation et l'introduction de nouveaux modèles d'entreprise.

Le leadership du continent révèle un support solide pour la priorisation et l'accélération de la numérisation. La stratégie de transformation numérique de l'Union africaine (UA), adoptée par le sommet de l'UA en février 2020, réclame, entre autres recommandations, le développement d'approches et de politiques continentales sur des questions interdisciplinaires telles que la protection des données, l'identification numérique, la cybersécurité et les technologies émergentes. Le Cadre stratégique en matière des données de l'Union africaine, conçu en 2021 par un groupe de travail panafricain et adopté par le sommet de l'Union africaine de février 2022, définit une vision commune, des principes, des priorités stratégiques et des recommandations clés pour guider les États membres de l'UA dans le développement de leurs systèmes de données nationaux et de leurs capacités à utiliser efficacement les données et à tirer de la valeur des données générées par les citoyens, entités gouvernementales et industries. De plus, le Cadre vise à optimiser la circulation transfrontalière des données à travers l'Afrique, à renforcer et à harmoniser les cadres de gouvernance des données en Afrique et à créer ainsi un espace de données partagé et des normes capables de réguler la production et l'utilisation croissantes des données à travers le continent.

L'Accord sur la zone de libre-échange continentale africaine (Accord ZLECAf) ouvre des perspectives de coopération sur des aspects majeurs de la transformation numérique et de la politique en matière de données. L'adoption plus étendue des fondements numériques d'initiatives continentales, comme l'Accord ZLECAf, sera cruciale pour tirer les profits d'une coopération économique plus soutenue. Ceci peut être facilité par des règlements rendant obligatoire une meilleure interopérabilité des données dans tout le pays, créant ainsi une démarche continentale harmonisée vers l'économie numérique axée sur les données. Cette démarche doit tendre à établir un équilibre entre, d'une part, la promotion des avantages socio-économiques des échanges commerciaux numériques et du commerce électronique, et d'autre part, la garantie de la sécurité constante des informations sensibles ainsi que le respect des réglementations pertinentes sur la protection des données à caractère personnel. Les négociations permanentes du Protocole de l'Accord ZLECAf sur le commerce numérique ouvrent aux États membres de l'UA des perspectives uniques d'harmonisation des réglementations de l'économie numérique, y compris des réglementations sur les données, en vue de soutenir la croissance économique collective du point de vue commercial.

Dans ce contexte, cette note de politique vise à fournir un plan général de principes et de directives (recommandations comprises) pour promouvoir l'usage responsable, sécurisé et équitable des données dans les accords commerciaux, dans le cadre des négociations permanentes du Protocole de l'Accord ZLECAf sur le commerce numérique et des négociations éventuelles de l'Accord ZLECAf sur les services et biens numériques (la seconde phase). Plus important encore, le protocole sur le commerce numérique jettera les bases d'un marché numérique continental unique.

2. VUE D'ENSEMBLE DU PAYSAGE DE LA POLITIQUE MONDIALE EN MATIÈRE DE DONNÉES

2.1 TENDANCES DE LA GOUVERNANCE DE LA CIRCULATION DES DONNÉES

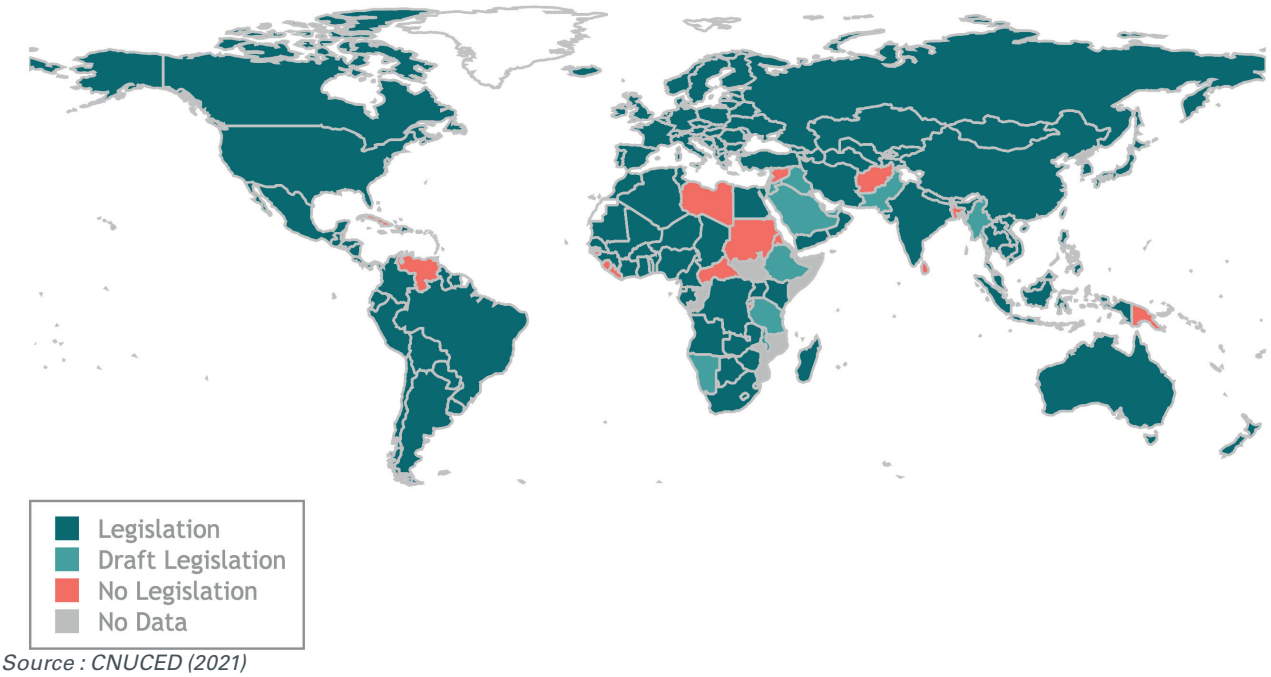
2.1.1. PAYSAGE DE LA GOUVERNANCE DES DONNÉES AUX NIVEAUX RÉGIONAL ET GLOBAL

Alors que les données font de plus en plus partie intégrante de la société contemporaine et que leur importance ne cesse de croître à l'ère numérique, le rôle d'une gouvernance efficace des données ne peut pas être sous-estimé. La gouvernance de la circulation des données est devenue une question essentielle. En effet, les données ont une valeur économique considérable et les informations sensibles méritent une utilisation et une protection appropriées. Par exemple, il y a eu diverses tendances dans la gouvernance de la circulation des données, chacune cherchant à relever les défis posés durant la collecte, le traitement, l'utilisation et la monétisation des données.

Les cadres de la gouvernance des données ont été motivés par le besoin de trouver un équilibre entre l'importance croissante des données en tant qu'atout, et la nécessité de protéger les droits à la vie privée de la personne. Il en résulte que des juridictions variées se concentrent diversement sur le règlement de questions liées aux données selon les points de vue des États au sujet de qui devrait « contrôler » les données. Actuellement, il y a par exemple trois orientations majeures des trois principaux territoires numériques. Les États-Unis se concentrent sur le contrôle des données par le secteur privé, la Chine met l'accent sur leur contrôle par le gouvernement tandis que l'Union européenne (UE) privilégie de contrôler des données par des individus sur la base des droits et valeurs fondamentaux (UNCTAD, 2021).

L'une des tendances prédominantes de la gouvernance de la circulation des données est l'adoption de lois sur la protection des données (UNCTAD, 2016). Les lois sur la protection des données visent à réglementer la collecte, le traitement et le stockage des données à caractère personnel (Crocetti, Peterson, & Hefner, n.d.). À partir de décembre 2021, environ 71 % des pays du monde ont mis en œuvre des lois sur la protection des données et la vie privée, tandis que 9 % ont des projets de loi (Figure 1) (UNCTAD, 2021). Dans l'ensemble, les lois et réglementations sur la protection des données varient d'un pays à l'autre. Dans le cas des États-Unis, par exemple, elles diffèrent d'un État à l'autre. Parmi toutes les législations sur la protection des données existantes, le Règlement général sur la protection des données de l'UE (RGPD) est considéré comme la batterie de règles les plus strictes sur la vie privée. Il a donné lieu à plusieurs lois sur la confidentialité des données semblables au RGPD (Satariano, 2018; Simmons, 2022).

Illustration 1. Législation internationale sur la protection des données et la vie privée, 2021



Source : CNUCED (2021)

En outre, il y a une convergence grandissante pour une transparence accrue dans la gouvernance de la circulation des données. Les attentes en faveur d'une transparence accentuée sur les pratiques concernant les données sont plus fortes, tant de la part des régulateurs que des consommateurs (Harvard Business Review, 2021). On attend des organisations qu'elles fournissent aux individus des informations claires sur le mode de collecte, de traitement et de stockage des données.

Nombreux sont les pays à introduire aussi de plus en plus des réglementations sur la localisation des données. Dans la mesure où des données peuvent être sensibles pour la sécurité nationale, on se préoccupe de plus en plus de la nécessité de stocker et de traiter des données dans les limites d'un pays (Yayboke & Ramos, 2021). Ainsi, certaines contrées introduisent des lois qui exigent que les données soient entreposées au sein de la juridiction où elles ont été collectées. Entre 2017 et 2021, le nombre de juridictions à détenir des lois sur la protection des données a connu une hausse substantielle, passant de 35 à 62. Ces 62 pays ont instauré 144 restrictions au total à propos de la localisation des données, contrairement à 2017 où seulement 67 mesures de cet ordre ont été mises en place (Cory & Dascoli, 2021).

Si elles sont jugées nécessaires pour des raisons de sécurité, les exigences de localisation des données peuvent constituer des obstacles au fonctionnement du commerce transfrontalier et des échanges internationaux (Hinrich Foundation, 2019). Les politiques de localisation des données augmentent par ailleurs le coût des transactions pour les entreprises étrangères, diminuant du même coup leur compétitivité internationale. Une étude de l'Information Technology and Innovation Foundation (ITIF) a découvert qu'un caractère restrictif croissant des données de 1 % peut entraîner 7 % de baisse de la production commerciale brute d'un pays, 2,9 % de baisse de productivité et une chute de 1,5 % des prix en aval (Cory & Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, 2021).

La localisation des données est étroitement liée à la souveraineté des données. Le concept de souveraineté des données préconise leur assujettissement aux lois et réglementations du pays où les données sont générées. La demande de souveraineté des données est guidée par des questions relatives au contrôle et à la propriété des données, particulièrement dans le contexte du cloud computing et de la circulation transfrontalière des données (Gao, 2022). Cette question est apparue essentiellement dans le contexte des groupes multinationaux capables de stocker des données en de multiples lieux. Certains pays ont adopté une position sur la souveraineté des données en instaurant des règles qui requièrent des entreprises qu'elles stockent les données localement et fournissent au gouvernement un accès plus grand à ces données (Kuo, 2022).

À l'autre bout du spectre, des initiatives ont vu le jour pour soutenir la libre circulation des données. Si les deux concepts ne sont pas forcément en contradiction, ils présentent des perspectives diverses des approches en matière de gouvernance des données. Dès 2000, la Déclaration conjointe sur le commerce électronique de l'Accord de libre-échange (ALE) entre les États-Unis et la Jordanie mettait déjà en lumière le « besoin de poursuivre la libre circulation des informations ». Depuis lors, un nombre croissant d'accords commerciaux régionaux (ACR) a intégré les mêmes aspirations et engagements. En 2019, l'initiative sur la Libre circulation des données en toute confiance (DFFT) fut proposée par le Japon et approuvée par des membres du G20 des nations (Kudo & Soble, 2022), tandis que l'UE a prôné une démarche plus prudente de promotion de la « libre circulation des données à caractère non personnel » (European Commission, 2023).

De surcroît, les données ouvertes, surtout les données gouvernementales, se sont focalisées sur la transparence et les aspects propices à l'innovation des données. De plus en plus de pays et d'institutions admettent que les données constituent une ressource précieuse pouvant être exploitée pour stimuler l'innovation et créer des opportunités nouvelles (World Bank, n.d.). À ce titre, ils préconisent que les données non sensibles et à caractère non personnel soient accessibles gratuitement et exploitables. De nombreux gouvernements dans le monde donnent de plus en plus accès à leurs données au public, les rendant ainsi disponibles pour un usage par différentes parties prenantes (OECD, 2020). C'est ainsi que le gouvernement du R.-U. a lancé data.gov.uk. Il s'agit d'un portail en ligne comportant des données publiées par le gouvernement central, les autorités locales et des services publics britanniques sur tout un éventail de secteurs et de sujets, y compris l'économie, la santé, le transport et l'éducation, entre autres (data.gov.uk, n.d.).

Eu égard aux diverses approches de la gouvernance des données, les entreprises qui se lancent dans le commerce international peuvent ainsi être confrontées à des difficultés et des coûts croissants de mise en conformité dans des juridictions multiples. Pour atténuer les défis imposés par des réglementations variées, il est important que des pays s'engagent dans le développement et l'adoption de normes internationales en matière de gouvernance des données susceptibles de les aider à simplifier et à harmoniser les réglementations. Un grand nombre de cadres internationaux, demeurant facultatifs pour la plupart, a été conçu à cet égard pour prodiguer des conseils sur les meilleures pratiques de gouvernance des données. Certains des cadres les plus significatifs adoptés à l'échelle internationale sont présentés cidessous. Une analyse plus exhaustive des meilleures pratiques est fournie à l'Annexe 2.

Les Nations unies (ONU) ont mis au point une série de principes sur la confidentialité des données. Ils visent à promouvoir l'utilisation responsable des données pour le développement durable tout en préservant la vie privée et en protégeant les droits de l'homme (UN Global Pulse, n.d.). Ceux-ci comprennent les principes des Nations unies relatifs à la protection des

données à caractère personnel et de la vie privée de 2018 (les « Principes ») ainsi que la Note d'orientation des Nations unies concernant les mégadonnées à l'appui de la réalisation de l'Agenda 2030 : confidentialité des données, éthique et protection (la « Note d'orientation »). Objectifs de ces Principes : i) harmoniser les normes de protection des données à caractère personnel dans le système des Nations unies ; ii) faciliter le traitement responsable de données à caractère personnel ; et iii) garantir le respect des droits de l'homme et des libertés fondamentales des individus, en particulier le droit à la vie privée. Ces Principes peuvent aussi servir de référence pour le traitement de données à caractère non personnel (United Nations, 2018).

Les lignes directrices de l'Organisation de développement et de coopération économiques (OCDE) régissant la protection de la vie privée constituent également un cadre international important pour la protection des données. Les lignes directrices de l'OCDE régissant la protection de la vie privée ont initialement été adoptées en 1980 pour orienter le traitement responsable des données à caractère personnel. Depuis lors, elles ont été mises à jour et révisées afin de se conformer à l'évolution rapide de l'environnement de la confidentialité des données (OECD, n.d.). Les lignes directrices de l'OCDE régissant la protection de la vie privée reposent sur certains principes fondamentaux ayant trait à l'importance de la qualité des données, aux spécifications des finalités, à la responsabilité et aux droits individuels (OECD, 2013). L'une des caractéristiques clés des lignes directrices de l'OCDE régissant la protection de la vie privée est l'accent qu'elles mettent sur la circulation transfrontalière des données. Les lignes directrices de l'OCDE régissant la protection de la vie privée insistent sur l'importance d'adopter des lois exhaustives sur la protection des données. Celles-ci doivent inclure des dispositions sur les transferts transfrontaliers de données, qui doivent être assorties de mesures de protection appropriées. En outre, ces lignes directrices spécifient que toute restriction imposée à la circulation transfrontalière de données doit être proportionnelle aux risques (OECD, 2013).

Le Cadre de protection de la vie privée de l'APEC fournit des principes sur la collecte, la détention, le traitement, l'utilisation, le transfert ou la divulgation d'informations personnelles appliquées à des personnes ou organisations des secteurs public et privé qui contrôlent chacun des processus susmentionnés. Ce Cadre favorise une approche flexible de la protection de la confidentialité des informations parmi les économies membres de l'APEC, en évitant la création d'obstacles inutiles pour la circulation des données (APEC, 2005). En mettant en œuvre le Cadre de protection de la vie privée de l'APEC, le système des Règles de confidentialité transfrontalières de l'APEC (CBPR) procure une certification sur la confidentialité des données soutenue par le gouvernement. Les entreprises peuvent y adhérer pour prouver qu'elles se conforment aux dispositifs de protection de la confidentialité des données reconnus à l'échelle internationale (APEC, 2019). Le système CBPR requiert des entreprises participantes qu'elles conçoivent et mettent en œuvre des politiques de confidentialité des données conformes au Cadre de protection de la vie privée de l'APEC.

Une initiative plus récente – la libre circulation des données en toute confiance (DFTT) du Forum économique mondial (FEM) – vise à faciliter le libre flux des données en garantissant la confidentialité et la sécurité des données. L'initiative DFFT est fondée sur le postulat que la libre circulation des données est essentielle à la croissance économique et à l'innovation, et que la protection et la confidentialité des données sont capitales au maintien de la confiance dans l'économie numérique (WEF, 2020). De ce fait, l'initiative tend à trouver un équilibre entre la promotion de la libre circulation des données et la protection des informations personnelles. Une feuille de route pour la coopération a été adoptée en 2021, avec notamment pour priorités quatre domaines de coopération : localisation des données, coopération réglementaire,

accès des gouvernements aux données et partage des données pour des secteurs prioritaires (Arasasingham & Goodman, 2023). En outre, un plan d'action a été établi en 2022. Étant donné sa portée internationale et l'accent mis sur le secteur privé, l'initiative pourrait contribuer à réduire la fragmentation des exigences réglementaires à l'échelle internationale, ce qui simplifierait l'accessibilité des entreprises aux données et leur utilisation au-delà des frontières.

Le RGPD de l'UE est un règlement exhaustif et rigoureux sur la protection des données à caractère personnel. En raison de sa portée, le RGPD a servi d'inspiration à l'élaboration de réglementations dans le monde entier. Le RGPD de l'UE est appliqué hors du territoire européen, requiert un consentement relatif au traitement, à la collecte et à l'utilisation des informations portant sur des sujets de l'UE, reconnaît les droits de confidentialité des personnes concernées et prévoit des sanctions en cas de non-conformité. Le RGPD de l'UE impose aussi certaines restrictions sur la circulation transfrontalière des données à caractère personnel. Suivant les dispositions du RGPD, le transfert de données à caractère personnel vers des pays présentant un niveau de protection approprié est garanti dans le cadre de la législation nationale. La Commission européenne est chargée de définir l'adéquation du niveau de protection des données dans les pays non membres de l'UE. Seuls quelques pays sont reconnus comme disposant de réglementations adéquates (European Commission, n.d.).[2] En l'absence de cette adéquation, des organisations recourent à d'autres mécanismes légaux pour transférer des données à caractère personnel hors de l'UE. Ceux-ci peuvent comprendre des clauses contractuelles types, des règles d'entreprise contraignantes, des codes de conduite et des dispositifs de certification (Commission européenne, n.d.).

Le développement solide de législations sur la protection des données traduit le rôle capital des données et de la circulation des données dans l'économie. Dans la société moderne, les données sont le moteur de « l'innovation disruptive axée sur les données » et de modèles d'entreprise rentables, tels que les entreprises plateformes ou les agrégateurs de données (Thirani & Gupta, 2017; Redman, 2015). Outre ses avantages économiques, le rôle des données outrepasse la perspective relativement étroite des modèles commerciaux d'une entreprise pour aborder les multiples facettes de la société, telles que la vie privée et la sécurité. Dans ce contexte, il faut une approche équilibrée pour garantir que les avantages économiques de l'innovation axée sur les données sont bien compris, tandis que la sécurité sociale et la vie privée continuent à bénéficier d'une protection appropriée. Le chapitre suivant abordera les nombreuses actions entreprises aux niveaux multilatéral, régional et national pour atteindre ce point d'équilibre.

2.1.1.1 ACCORDS COMMERCIAUX RÉGIONAUX ET MULTILATÉRAUX INCLUANT DES DISPOSITIONS SUR LES DONNÉES

(I) DISCIPLINES DE L'OMC CONCERNANT LA QUESTION DES DONNÉES

Tout en étant considérée comme une « *réglementation antérieure à Internet* », les règles multilatérales existantes de l'OMC conservent une certaine applicabilité sur les mesures de gouvernance des données. Le principe de neutralité technologique fournit une base importante pour l'application au commerce électronique des règles relatives au GATS existantes (Mattoo

2 Les pays reconnus par la Commission de l'UE comme disposant de règlements adéquats sur la protection des données incluent Andorre, l'Argentine, le Canada (organisations commerciales), les îles Féroé, Guernesey, Israël, l'Île de Man, le Japon, Jersey, la Nouvelle-Zélande, la République de Corée, la Suisse, le Royaume-Uni et l'Uruguay.

& Schuknecht, 1999). Fondamentalement, ce principe tend à garantir l'absence de distinction de politique entre les produits basés sur les vecteurs, ouvrant ainsi la porte à la longévité et à l'égale application d'un règlement à des technologies différentes (Greenberg, 2016). Un rapport du Conseil du commerce des services (1999) de l'OMC prévoit que « *les Membres ont accepté que le GATS [Accord général sur le commerce des services] s'applique à l'ensemble des services, quels que soient les moyens technologiques par lesquels ils ont été fournis. ... Il est apparu que le principe de neutralité technologique s'est appliqué également aux engagements programmés, sauf autre spécification du programme : des Membres ont donc pu planifier des engagements de manière non technologiquement neutre* » (WTO, 1999). Le rapport de suivi de l'OMC pour le Programme de travail sur le commerce électronique confirme également la neutralité technologique du GATS « dans le sens où il ne contient aucune disposition faisant la distinction entre les différents moyens technologiques par lesquels un service peut être fourni » (WTO, 1999). Voilà qui donne une raison importante de lire les programmes d'engagements des Membres de l'OMC : restriction ou interdiction de la circulation transfrontalière des données, entravant ainsi la fourniture transfrontalière de services dans des secteurs où des membres ont pris des engagements GATS explicites susceptibles d'enfreindre l'obligation d'accès au marché (Mitchell & Hepburn, 2017).

L'Accord général sur le commerce des services (GATS) de l'OMC fournit une raison importante d'imposer des mesures légitimes de protection des données à caractère personnel et de la vie privée. En particulier, l'article XIV c) i) reconnaît l'importance de la protection de la vie privée et permet en conséquence que des Membres dérogent à leurs obligations existantes lorsque cela est nécessaire à la protection de la vie privée des personnes pour ce qui est du traitement et de la dissémination de données à caractère personnel.[3] L'exception portant sur la « moralité publique » visée à l'article XIV a) du GATS peut aussi être interprétée pour protéger la vie privée. Par ailleurs, l'Annexe sur les télécommunications du GATS permet de prendre les mesures « nécessaires pour assurer la sécurité et la confidentialité des messages. »[4] D'une manière générale pour toutes les exceptions du GATS, ces mesures ne doivent pas être adoptées sur une base discriminatoire ou à des fins de protectionnisme. Il est également bon de noter toutefois que le GATS n'aborde pas spécifiquement la protection des données et informations à caractère personnel, ce qui donne lieu à de graves lacunes dans ce régime commercial international à l'ère numérique.

En l'absence de règles explicites pour le commerce numérique dans les accords de l'OMC, la Déclaration conjointe sur l'Initiative (JSI) relative au commerce électronique présente une étape vers une discipline concernant la gouvernance des données. À la 11e Conférence ministérielle, en 2017, 76 Membres de l'OMC ont convenu d'entreprendre des travaux exploratoires en vue de futures négociations sur les aspects du commerce électronique, gouvernance des données comprise. Le projet de texte de négociation consolidé de la JSI se concentre sur six aspects clés présentés dans Figure 2. Fin mars 2023, les participants impliqués dans l'initiative ont convenu de débattre de diverses propositions relatives au commerce électronique, circulation des données incluse (WTO, 2023). Une déclaration antérieure avait indiqué que les

3 Article XIV c) i) du GATS : « Aucune disposition du présent Accord n'est interprétée comme empêchant l'adoption ou l'application par tout Membre de mesures : c) nécessaires pour assurer le respect des lois ou réglementations qui sont compatibles avec les dispositions du présent Accord, y compris celles qui se rapportent : i) à la protection de la vie privée des personnes pour ce qui est du traitement et de la dissémination des données à caractère personnel, ainsi qu'à la protection de la confidentialité des dossiers et comptes personnels. »

4 Le paragraphe 5 d) de l'Annexe sur les télécommunications du GATS spécifie ce qui suit : « [Un] Membre peut prendre les mesures nécessaires pour assurer la sécurité et la confidentialité des messages, pour autant que ces mesures ne soient pas appliquées de façon à constituer soit un moyen de discrimination arbitraire ou injustifiable, soit une restriction déguisée au commerce des services ».

Membres étaient parvenus à un consensus appréciable sur des aspects tels que la protection des consommateurs en ligne, les messages électroniques commerciaux non sollicités, les données gouvernementales ouvertes et le libre accès à Internet (WTO, 2021). En attendant, les Membres cherchent encore une ligne de convergence sur des thèmes comme la protection des données et la vie privée, la circulation transfrontalière des données, le code source et la cryptographie (WTO, 2023). Le même bras de fer sur les questions de gouvernance des données figure dans les négociations de l'Accord sur le commerce des services (TiSA). D'une part, les États-Unis qui défendent le transfert transfrontalier de données, y compris de données à caractère personnel, en lien avec la conduite de l'entreprise du prestataire de services (Berka, 2017). L'UE, d'autre part, qui s'oppose à cette proposition au motif que « le droit à la vie privée devra être reconnu comme un droit fondamental, non comme une barrière commerciale » et qui promeut le système d'adéquation (European Parliament, 2016).

Illustration 2. Aspects clés des négociations JSI sur le commerce électronique de l'OMC

PERMETTRE LE COMMERCE ÉLECTRONIQUE
- Faciliter les transactions électroniques
- Facilitation du commerce numérique et logistique

OUVERTURE ET COMMERCE ÉLECTRONIQUE
- Non-discrimination et responsabilité
- Droits de douane sur les transmissions électroniques
- Circulation des informations
- Accès à Internet et aux données

CONFIANCE ET COMMERCE ÉLECTRONIQUE
- Protection des consommateurs
- Confidentialité
- Confiance des entreprises

QUESTIONS INTERSECTORIELLES
- Transparence, réglementation nationale et coopération
- Cybersécurité
- Renforcement des capacités

TÉLÉCOMMUNICATIONS
- Mise à jour du document de référence de l'OMC sur les services de télécommunication
- Équipements réseau et produits

ACCÈS AU MARCHÉ
- Accès au marché des services
- Admission et séjour temporaires du personnel lié au commerce électronique
- Marché des biens

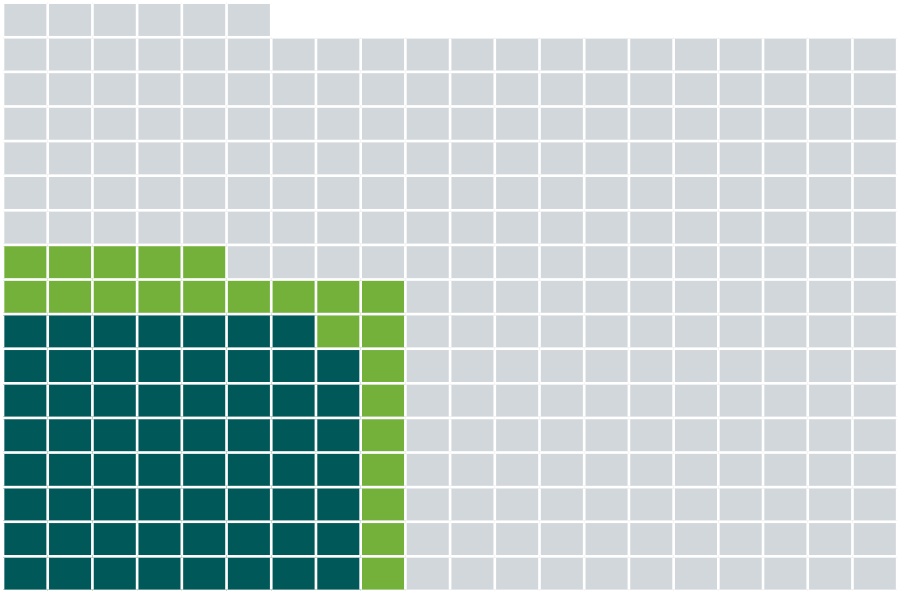
Source : (WTO Plurilaterals, n.d.)

(II) DISPOSITIONS CLÉS RELATIVES AUX DONNÉES DES ACR

Un nombre grandissant d'accords commerciaux régionaux (ACR) comprend des dispositions sur le commerce numérique et intègre aussi consécutivement certaines clauses afférentes aux données. Dans une étude récente, Burri (2021) constate que 184 des 347 ACR conclus entre 2000 et 2019 incluaient des dispositions sur le commerce numérique, représentant ainsi plus de la moitié des accords commerciaux régionaux signés sur cette période (Burri, Big Data and Global Trade Law, 2021). L'inclusion de ces dispositions a encore progressé de 2010 à ce jour, 68 % de tous les ACR signés entre 2010 et 2019, intégrant certains types de disposition sur le commerce numérique. De même, au fil des années, le nombre de dispositions intégrées à ces paragraphes a augmenté. Par exemple, en 2000, le nombre moyen d'articles concernant le commerce numérique était d'un. En 2019, le nombre moyen d'articles concernant le commerce numérique est passé à treize (Burri, Big Data and Global Trade Law, 2021). Il convient cependant de noter que les dispositions figurant dans ces paragraphes sont extrêmement variées et abordent une série de thèmes différents allant du commerce électronique à la protection des données en passant par le commerce dématérialisé. En outre, il a été constaté aussi que le degré d'exécution de ces dispositions varie entre les accords.

Les dispositions relatives aux données constituent un phénomène relativement nouveau pour les ACR. Les États-Unis ont joué un rôle notable dans l'intégration de dispositions sur les données dans leurs ACR, en prônant des règles libérales à la lumière de leur « Stratégie numérique » (Burri, Big Data and Global Trade Law, 2021). Parmi les accords passés avec l'Australie, Bahreïn, le Chili, le Maroc, Oman, le Pérou, Singapour, le Panama, la Colombie et la Corée du Sud, tous contenaient des clauses concernant le commerce numérique selon lesquelles les États-Unis sont allés au-delà des engagements de l'OMC sur la question. Il n'en demeure pas moins que d'autres pays, notamment Singapour, l'Australie, le Japon et la Colombie, ont joué un rôle tout aussi déterminant dans la diffusion de ces dispositions dans les ACR (Burri, Big Data and Global Trade Law, 2021). Jusqu'en 2020, selon la base de données DESTA, soixante-trois des 346 ACR signés depuis 2000 (soit 18 % de l'ensemble) intègrent des dispositions relatives aux données (Figure 3). Au fil des ans, le nombre d'ALE (accords de libre-échange), comptant des dispositions sur le commerce électronique, reste plus élevé que ceux avec des clauses sur les données, ce qui révèle la réticence continue des pays à intégrer des règlements de gouvernance des données dans les accords commerciaux.

Illustration 3. Couverture des données et du commerce électronique de tous les ALE signés depuis 2000



25%
(**86** hors de 346)
de l'ALE couvre les dispositions relatives au commerce électronique.

18%
(**63** hors de346)
de l'ALE couvre les dispositions relatives aux données. Ils couvrent également les dispositions relatives au commerce électronique.

ALE qui comprend uniquement des dispositions sur le commerce électronique.

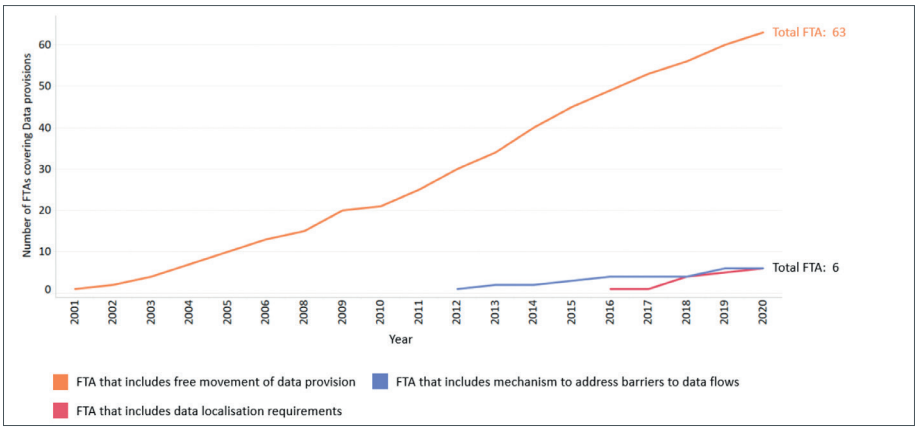
ALE qui comprend à la fois des dispositions sur les données et le commerce électronique.

ALE qui n'inclut pas de dispositions sur les données et le commerce électronique.

Source : Calculs de l'auteur à partir de (Dür, Baccini, & Elsig, 2022)

Si la clause de libre circulation des données est incluse depuis 2001, ce n'est qu'en 2012 qu'ont commencé à apparaître des dispositions pour des mécanismes de suppression des obstacles à la circulation des données. La première inclusion fut l'accord de l'Alliance du Pacifique. Fin 2020, six accords similaires à travers le monde comprenaient des clauses de suppression des obstacles à la circulation des données. Il s'agissait des accords Alliance du Pacifique, UE-Colombie et Pérou, Mexique-Panama, Japon-Mongolie, Argentine-Chili et UE-Japon. À partir de 2016, on a commencé à intégrer dans les ALE des exigences portant sur la localisation des données. Le premier accord concerné fut l'accord Japon-Mongolie, entré en vigueur en 2016. À la fin de 2020, six accords mentionnaient des exigences relatives à la localisation des données (Figure 4).

Illustration 4. FTA contenant des dispositions relatives aux données et entrés en vigueur depuis 2000, par type de couverture



Source : Calculs de l'auteur à partir de (Dür, Baccini, & Elsig, 2022)

(III) EXAMEN DÉTAILLÉ DES DISPOSITIONS RELATIVES AUX DONNÉES DANS LES ACR SÉLECTIONNÉS

Ce chapitre évalue quelques-uns des accords les plus récents et exhaustifs qui intègrent des dispositions de gouvernance des données. 6 ACR au total ont été évalués au regard de 14 types de disposition différents. Table 1 met en exergue la couverture des diverses dispositions relatives aux données intégrées aux ACR sélectionnés.

Tableau 1. Couverture des différentes dispositions relatives aux données dans les ACR

Agreements	Cross Border Data Flows	Data Localisation	Data Protection	Digital Identities	Open Government Data	Data Innovation	Digital Inclusion	Cooperation	Cybersecurity	Cryptography	Source Code	Online Safety & Security	Spam
CPTPP	Y	Y	Y	N	N	N	N	Y	Y	N	Y	Y	Y
DEPA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
EU-UK TCA	Y	N	Y	N	Y	N	N	Y	Y	N	Y	Y	Y
UK-Singapore DEA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
USMCA	Y	Y	Y	N	Y	N	N	Y	Y	N	Y	Y	Y
RCEP	Y	Y	Y	N	N	N	N	Y	Y	N	N	Y	Y

N	The Agreement does not include a specific provision on the subject
Y	The Agreement includes a specific provision on the subject
	Data governance provisions
	Provisions related to responsible, secure and equitable use of data

*Spam or also Unsolicited Commercial Electronic Messages

Source : Compilation de l'auteur

En termes de couverture, on constate que les six ACR sélectionnés comprennent tous des dispositions de gouvernance des données. Le Partenariat numérique R.-U.-Singapour (DEA) est l'accord le plus ambitieux étudié dans le cadre de ce rapport, puisqu'il couvre l'ensemble des 14 différents types de provision faisant l'objet de l'évaluation. Il est suivi de l'Accord de partenariat sur l'économie numérique (APEN), qui inclue 13 des 14 types de disposition afférente aux données. Le seul aspect non couvert par l'APEN, dans ce cas, concerne des dispositions sur le code source. A contrario, les accords mentionnant le moins de dispositions

sur les données sont l'Accord de commerce et de coopération (ACC) entre le Royaume-Uni et l'Union européenne et le Partenariat économique régional global (RCEP), avec seulement 8 aspects couverts dans chacun.

La libre circulation des informations figure, en tant que disposition majeure, dans tous les ACR. On peut remonter à l'ALE Jordanie-É.-U. de 2000 pour trouver la première mention de la libre circulation des informations dans un ALE. La déclaration conjointe sur le commerce électronique y exprimait la « nécessité de poursuivre la libre circulation des informations » (Burri, Big Data and Global Trade Law, 2021). Des accords commerciaux récents mentionnent plus de dispositions de fond sur la libre circulation des informations. Selon l'Article 8.61F du Partenariat numérique R.-U.-Singapour (DEA), aucune des deux parties « *ne saura interdire ou restreindre le transfert transfrontalier d'informations par des moyens électroniques, y compris des informations sur le personnel, si cette activité est destinée à la conduite de l'entreprise d'une personne protégée*. » De son côté, l'Accord de partenariat transpacifique global et progressiste (CPTPP) déclare que « *chaque partie doit permettre le transfert transfrontalier d'informations par des moyens électroniques, y compris des informations sur le personnel, dès lors que cette activité sera destinée à la conduite de l'entreprise d'une personne protégée*. » Les formulations des quatre autres accords sont similaires à cet égard. Par conséquent, il existe une plus grande convergence sur l'adoption de dispositions contraignantes à cet effet.

À l'exception de l'ACC UE-R.-U., tous les accords évalués mentionnent des dispositions limitant l'application des exigences sur la localisation des données. Dans les cinq accords, il est interdit d'imposer des restrictions sur la localisation des données. Il est spécifié à l'article 4.4.2 de l'APEN que « *aucune partie ne saura exiger d'une personne protégée d'utiliser ou de placer des infrastructures informatiques sur le territoire de cette partie en tant que condition de la conduite de l'entreprise sur ledit territoire* », et la formulation linguistique mentionnée dans les autres accords est très semblable. En fait, la plupart des ACR comprenant des dispositions sur la localisation des données incluent un langage ferme et des engagements contraignants. Le premier accord à contenir des engagements contraignants sur la localisation des données fut l'ALE Japon–Mongolie signé en 2015. Les négociations sur le Partenariat transpacifique (PTP) ont considérablement influencé ces dispositions dans les accords ultérieurs, y compris notamment l'Accord de partenariat transpacifique global et progressiste (CPTPP) et l'Accord Canada-États-Unis-Mexique (ACEUM) (Burri, Big Data and Global Trade Law, 2021).

Pour ce qui concerne la protection des données à caractère personnel, cinq des six accords comportent des engagements contraignants. À part l'ACC UE-R.-U., les dispositions relatives à la protection des données à caractère personnel sont cohérentes dans tous les ACR. Par exemple, en vertu de l'article 19.8.2. de l'Accord Canada-États-Unis-Mexique (ACEUM), « *chaque partie doit adopter ou maintenir un cadre légal prévoyant la protection des informations personnelles des utilisateurs du commerce numérique*… ». La plupart des accords spécifient aussi que tout cadre légal adopté doit répondre aux normes et principes internationaux. Pour ce faire, l'ACEUM se réfère au Cadre de protection de la vie privée de l'APEC et à la Recommandation du Conseil de l'OCDE concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel (2013). En outre, les accords comprennent aussi des dispositions contraignantes requérant l'adoption de pratiques de protection non discriminatoires des utilisateurs du commerce numérique contre des infractions à la protection d'informations personnelles et la publication des protections des informations personnelles fournies aux utilisateurs du commerce numérique.

Hormis ces trois aspects clés de la gouvernance des données, de plus en plus d'ACR cherchent aussi à intégrer des dispositions visant à garantir l'utilisation responsable, sûre et équitable des données. Pour cette évaluation, 11 domaines différents ont été identifiés et évalués selon Table 1. Pour ce faire, les dispositions comprennent un mélange d'engagements à la fois contraignants et non contraignants. Par exemple, lorsqu'il est question du transfert et de l'accès à des codes sources, les quatre accords où le sujet est abordé incluent tous des engagements contraignants. Dans ce contexte, l'Accord de partenariat transpacifique (CPTPP) établit que « *aucune partie ne saura exiger le transfert du ou l'accès au code source du logiciel détenu par une personne d'une autre partie, en tant que condition à l'importation, la distribution, la vente ou l'exploitation de ce logiciel, voire de produits contenant ce logiciel, sur son territoire.* » À l'autre bout du spectre, les dispositions sur l'innovation numérique, que l'on trouve uniquement dans l'APEN et le DEA R.-U.-Singapour par exemple, sont des clauses d'effort maximal et par conséquent non contraignantes.

2.2 CADRE STRATÉGIQUE ET RÉGLEMENTAIRE DE L'UNION AFRICAINE SUR LA CIRCULATION DES DONNÉES

Le continent africain s'est engagé de manière proactive sur la voie de la transformation numérique. En 2020, le Sommet de l'UA a adopté la **stratégie de transformation numérique de l'UA (STN)** pour l'Afrique (2020-2030). Elle vise à accompagner une réponse africaine commune et coordonnée aux défis et aux opportunités de la Quatrième révolution industrielle (4IR) puisqu'elle expose la poursuite de ses objectifs d'accès universel aux réseaux numériques et la mise en place d'un marché numérique unique (MRD) d'ici 2030.

Conformément à la **stratégie de l'UA sur l'environnement politique et réglementaire favorable au marché unique numérique de l'Afrique**, le marché unique numérique est désigné comme l'un des trois piliers essentiels qui soutiennent l'accomplissement des MRD africains.[5] Pour tirer les bénéfices potentiels de l'existence d'un marché de données communes, tous les pays africains doivent posséder des cadres légaux propices en vue de permettre et de faciliter la libre circulation des données. Ces cadres sont essentiels au développement d'un marché de données communes en Afrique. En effet, ils fournissent les règles et textes législatifs nécessaires à la libre circulation transfrontière des données. Ces cadres sont indispensables pour garantir que des données peuvent être collectées, partagées et analysées sans porter atteinte aux droits individuels, aux questions de sécurité nationale ou aux lois sur la propriété intellectuelle. Du fait qu'ils procurent un ensemble clair et cohérent de règles et textes législatifs pour la collecte, le partage et l'analyse des données, ces cadres peuvent aider à libérer le potentiel de développement axé sur les données en Afrique. Les chapitres, sous-chapitres suivants 2.2.1 et 2.2.2, mettent en lumière certaines des avancées décisives réalisées à cet effet aux niveaux régional et national respectivement.

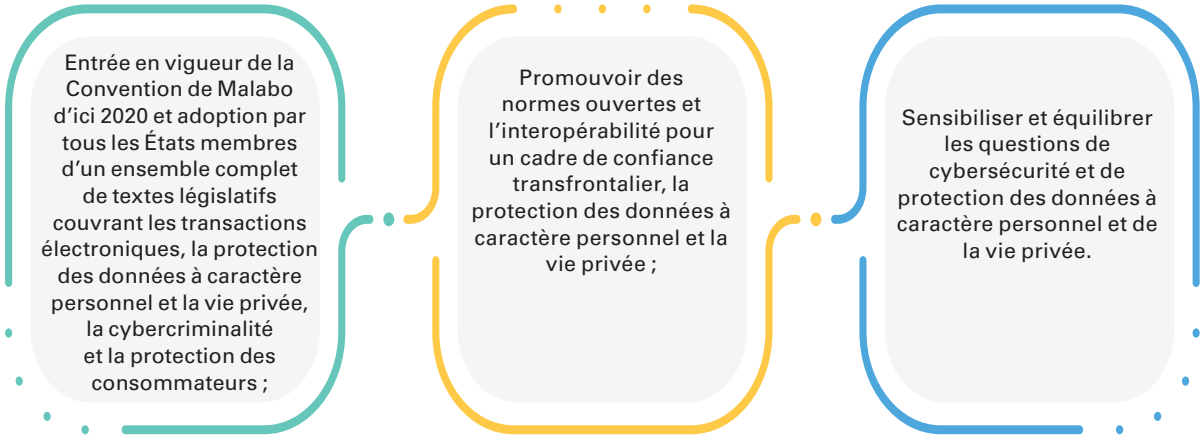
5 Les trois piliers sont les suivants : Marché de la connectivité unique ; Marché des données unique et Marché en ligne unique. Cf. (Stratégie de l'Union africaine sur l'environnement politique et réglementaire favorable au marché unique numérique de l'Afrique, adoptée par le sommet de l'UA en février 2024).

2.2.1 CADRES CONTINENTAUX ET RÉGIONAUX

(I) STRATÉGIE DE TRANSFORMATION NUMÉRIQUE POUR L'AFRIQUE

La Stratégie de transformation numérique pour l'Afrique (STN) (2020-2030) est l'instrument clé d'orientation de l'engagement du continent sur la voie numérique. La STN, approuvée lors de la 36e Session ordinaire du Conseil exécutif de l'Union africaine, vise à maîtriser les technologies et l'innovation numériques pour transformer les sociétés et les économies africaines en vue de promouvoir, entre autres, le développement socio-économique du continent et d'assurer l'appropriation par l'Afrique des outils modernes de gestion numérique (African Union, 2020). La STN définit le programme en faveur d'une plus grande cohérence des politiques et stratégies numériques existantes et futures, en vue de positionner l'Afrique en tant que partenaire stratégique de l'économie numérique globale. En reconnaissant les données comme une force motrice cruciale de la transformation numérique, de l'intégration, de l'innovation et de l'entrepreneuriat, du commerce et des services financiers, la STN a pris note des défis liés au développement et à l'utilisation de bonnes données et a proposé diverses recommandations et mesures politiques en vue d'améliorer l'accès et l'utilisation des données. Quelques-uns des objectifs spécifiques de la STN concernant la gouvernance des données sont exposés ci-dessous.

Illustration 5. Les objectifs spécifiques de la STN relatifs à la gouvernance des données



Source: (African Union, 2020)

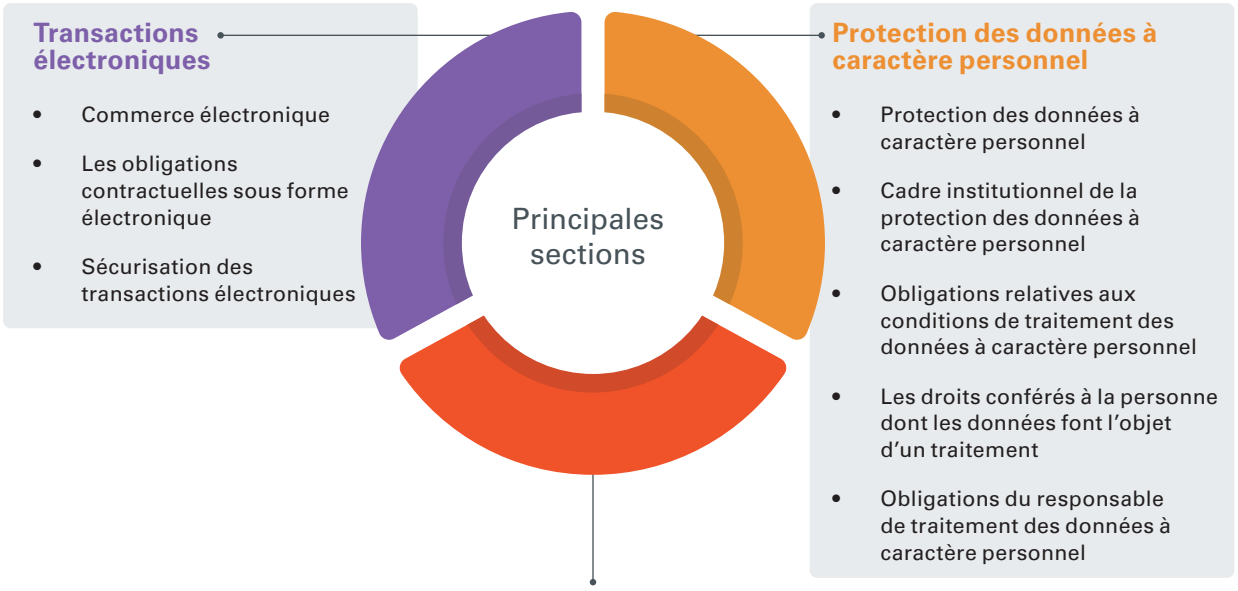
La STN présente une feuille de route ambitieuse en matière de gouvernance et de protection des données. L'une des recommandations proposées suivant la STN vise à garantir la cohérence de la Convention de Malabo avec les normes internationales pour confirmer la compétitivité des entreprises africaines sur les marchés internationaux. L'instrument définit l'objectif d'établir des réglementations dans 10 des 14 aspects liés aux données (comme précisé au chapitre 2.1.2). Les seuls aspects pour lesquels la STN ne dispose d'aucun détail sur le transfert et l'accès au code source dans les flux transfrontaliers, les messages commerciaux non sollicités, les produits utilisant la cryptographie et l'innovation en matière de données. Ainsi, en cas de mise en œuvre et d'exécution adéquates, les objectifs de la STN aboutiraient à un paysage réglementaire assez solide pour les pays africains. Dans ce sens, la portée et la couverture ambitieuses de la STN peuvent servir de lignes directrices importantes pour les négociateurs, dans le cadre de la négociation de dispositions relatives aux données dans le contexte du protocole de l'Accord ZLECAf sur le commerce numérique.

(II) CONVENTION DE MALABO

Au cours de la décennie passée, l'Afrique a assisté au développement de divers instruments de gouvernance permettant d'aborder et de faciliter la création et le renforcement d'écosystèmes numériques africains. En juin 2014, l'Union africaine a adopté la Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données à caractère personnel (dite Convention de Malabo) pour instaurer un cadre crédible pour la cybersécurité et la protection des données en Afrique. La Convention de Malabo est née à la lumière de l'importance croissante des données et technologies numériques en Afrique et du besoin de cadres légaux globaux pour régir leur utilisation. La Convention de Malabo vise à déterminer « *les règles essentielles à la mise en place d'un environnement numérique crédible (cyberespace) et à pallier les insuffisances qui affectent la réglementation en matière de reconnaissance juridique des communications de données et de la signature électronique, ainsi que l'absence de règles juridiques spécifiques visant à protéger les consommateurs, les droits de propriété intellectuelle, les données à caractère personnel et les systèmes d'information et de la confidentialité en ligne* » (African Union Commission, 2018).

La Convention se concentre sur trois aspects clés, notamment les transactions électroniques, la protection des données à caractère personnel, les cybersécurité et cybercriminalité. La Convention serait fondamentale dans le développement de normes communes promouvant et régulant l'utilisation des données sur le continent. La Convention fournit aux pays un cadre juridique commun et vise à établir un écosystème propice à la transmission et au partage transfrontalier des données. Les divers chapitres de la Convention sont résumés ci-dessous. De plus, la Convention reconnaît également l'importance de la circulation transfrontalière des données pour le développement économique en Afrique. Elle permet la libre circulation transfrontière des données, sous réserve de garanties appropriées pour la protection des données et la cybersécurité. La Convention exige par ailleurs que les pays mettent en place des mécanismes de reconnaissance de normes de protection des données et de résolution des différends inhérents à la circulation transfrontalière des données.

Illustration 6. Principales sections de la Convention de Malabo



Source: (African Union Commission, 2018)

La ratification de la Convention de Malabo a pris du temps en raison de nombreux facteurs. À partir de mai 2023, 19 sur 55 États membres africains ont signé la convention, 15 d'entre eux ayant procédé aussi à sa ratification (African Union, 2023). La dernière ratification a été opérée par la Mauritanie le 9 mai 2023, ce qui a déclenché l'entrée en vigueur de la convention le 8 juin 2023 (Ayalew, 2023)[6] L'un des principaux motifs des retards liés à la ratification et à la mise en œuvre de la Convention pourrait être attribué au manque de dynamisme et de volonté politique parmi les pays africains, beaucoup ayant déjà instauré des réglementations et normes nationales sur la gouvernance des données (Okwara, 2022). De plus, on a assisté à un manque de sensibilisation de la Convention dans des pays africains, où elle a fait l'objet de mesures marketing et d'un élan insuffisants une fois adoptée en 2014. L'élaboration du Protocole de l'Accord ZLECAf sur le commerce numérique permet de promouvoir à nouveau la ratification de la Convention de Malabo. En effet, elle a le potentiel adapté pour fournir des conseils et des orientations sur les problèmes et défis émanant du commerce numérique.

6 Parmi les pays qui ont ratifié la Convention figurent l'Angola, le Cap-Vert, la Côte d'Ivoire, le Congo, le Ghana, la Guinée, le Mozambique, la Mauritanie, Maurice, la Namibie, le Niger, le Rwanda, le Sénégal, leTogo et la Zambie.

(III) LE CADRE STRATÉGIQUE EN MATIÈRE DES DONNÉES DE L'UNION AFRICAINE

Le Cadre stratégique en matière des données de l'Union africaine représente un développement important concernant la gouvernance des données sur le continent africain. Le Cadre stratégique en matière des données de l'UA a été conçu en reconnaissance des opportunités présentées par la STN et l'Accord ZLECAf pour aborder et maîtriser la croissance des données que permettra l'économie numérique de l'Afrique (African Union, 2022). Le Cadre stratégique représente une étape importante vers la création d'un environnement de données consolidé et de systèmes harmonisés de gouvernance des données numériques, afin de permettre la circulation libre et sécurisée des données sur le continent tout en préservant les droits de l'homme, en garantissant la sécurité et un accès équitable aux avantages, tout comme leur partage.

Ce Cadre définit une vision commune, des principes, des priorités stratégiques et des recommandations clés pour guider les pays africains dans le développement de leurs systèmes de données nationaux et de leurs capacités à utiliser efficacement les données et à en tirer de la valeur. Il reconnaît les données comme un prérequis pour la création de valeur, l'esprit d'entreprise et l'innovation en Afrique (African Union, 2022). En vue de développer et de maîtriser les données en Afrique, le Cadre propose l'alignement de la création et du développement des données sur tout le continent avec les principes de coopération, d'intégration, d'équité et d'inclusivité, de confiance, de sécurité et de responsabilité, d'exhaustivité et d'anticipation ainsi que d'intégrité et de justice. En tant que tel, une fois mis en œuvre, le Cadre :

1. donnera aux Africains les moyens d'exercer leurs droits par la promotion de systèmes de données fiables, sûrs et sécurisés, qui seront intégrés sur la base de normes et de pratiques communes ;
2. créera, coordonnera et donnera les moyens aux institutions de gouvernance de réguler, si nécessaire, le paysage des données en constante évolution et d'accroître l'utilisation productive et innovante des données afin de fournir des solutions et de créer de nouvelles opportunités tout en atténuant les risques ; et
3. veillera à ce que les données puissent traverser les frontières aussi librement que possible, tout en réalisant une distribution équitable des bénéfices et en traitant les risques liés aux droits de l'homme et à la sécurité nationale (African Union, 2022).

Le Cadre propose en outre que les modèles de données et de sécurité soient impérativement transversaux, avec un accent particulier sur le stockage et le traitement en nuage des données sensibles/propriétaires, la gestion des API et le soutien des marchés de données équitables (African Union, 2022). Le Cadre présente un ensemble de recommandations détaillées et de mesures connexes pour guider les États membres dans la formulation des politiques dans leur contexte national ainsi que des recommandations pour renforcer la coopération entre les pays et promouvoir les flux de données intra-africains.

(IV) CADRE D'INTEROPÉRABILITÉ DES SYSTÈMES D'IDENTIFICATION NUMÉRIQUE

Le Cadre d'interopérabilité des systèmes d'identification numérique est un cadre connexe développé aussi par l'Union africaine. Les identifications numériques présentent de nombreux avantages pour une société dans laquelle gouvernements et entreprises, par exemple, peuvent les utiliser pour rationaliser, étendre leurs opérations et faire preuve d'innovation en matière de transactions ainsi que pour améliorer la fourniture de services par la numérisation et l'automatisation, notamment lorsqu'on les envisage comme un « empilement

numérique » avec des plateformes de paiement numérique et de partage de données fiables. Le Cadre prévoit une norme commune au niveau continental pour représenter, sous une forme numérique, les preuves d'identité émises par des sources de confiance d'États membres de l'UA et pour assurer l'interopérabilité sur tout le continent. Le Cadre sera essentiel à la facilitation du commerce numérique en autorisant l'usage d'identités numériques fiables et authentifiées, et permettra la création d'ensembles de données capables de soutenir le développement d'autres services en Afrique.

(V) INITIATIVES POUR DES LOIS TYPES RÉGIONALES

Au niveau régional, de nombreuses communautés économiques régionales africaines (CER) ont également mis au point des instruments destinés à réguler l'utilisation et le stockage de données dans leurs États membres. Ceux-ci comptent le Cadre juridique de la Communauté économique d'Afrique de l'Est (CAE) pour la cyberlégislation de 2008 ; la Loi complémentaire sur la protection des données à caractère personnel de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) ; les Lois types relatives aux télécommunications/TIC et la cybersécurité qui intègrent des dispositions sur la protection des données, la cybercriminalité et les transactions électroniques dans la région CEEAC (Communauté économique des États de l'Afrique centrale) ; et les Lois types de la Communauté de développement de l'Afrique australe (SADC) sur le commerce électronique / les transactions électroniques, la protection des données, la cybercriminalité, etc.

Le Cadre juridique de la CAE pour la cyberlégislation de 2008 fut parmi les premières initiatives en Afrique à adopter un cadre harmonisé efficace et moderne à l'échelle régionale pour la cyberlégislation. Ce cadre a été conçu pour répondre aux besoins de la région de soutenir le processus d'intégration régional en matière de gouvernement et de commerce électroniques (UNCTAD, 2012). Le cadre comprend deux volets de documents : Le cadre I concerne les transactions électroniques, y compris les signatures électroniques ; la cybercriminalité ; la protection des données et de la vie privée ; la protection des consommateurs. Le cadre II concerne la propriété intellectuelle ; la concurrence ; la fiscalité numérique et la sécurité de l'information. Il n'en demeure pas moins que la transposition de ces cadres et règles exigera des travaux complémentaires pour veiller à l'alignement et à l'application au niveau national. Sur les six États membres de la CAE, seul le Rwanda a signé et ratifié la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel.

La Loi complémentaire sur la protection des données à caractère personnel de la CEDEAO, signée le 16 février 2010, vise à établir un cadre légal harmonisé pour le traitement de données à caractère personnel dans ses États membres. La présente loi est juridiquement contraignante, et il est demandé aux États membres de la mettre en œuvre dans un délai de deux ans à partir de son adoption. En conséquence, chaque État membre a l'obligation d'instaurer un cadre légal pour la protection des données à caractère personnel, relativement à la collecte, au traitement, à la transmission, au stockage et à l'utilisation des données à caractère personnel. En outre, chaque État membre doit créer une Autorité indépendante chargée de la protection des données (DPA), afin de veiller au traitement des données à caractère personnel en conformité avec les dispositions de la loi. Des sanctions administratives et financières sont également prévues pour parer aux violations des dispositions de la Loi par des responsables du traitement des données ou des informaticiens (OneTrust, 2022).

Créée en 2013, la Loi type sur la protection des données de la SADC sert de cadre général aux États de la région pour l'élaboration de leurs propres textes législatifs nationaux sur la protection des données. Elle concerne un large spectre de domaines différents, y compris l'instauration d'une autorité chargée de la protection des données, de lignes directrices sur la qualité des données, de règles générales sur le traitement des données à caractère personnel, les devoirs du responsable du traitement ou de l'informaticien en charge des données, les droits de la personne concernée, le recours aux autorités judiciaires, les sanctions et les flux transfrontaliers d'informations (ITU, 2013). Reposant sur des principes internationaux et compatibles avec la Convention de Malabo, les Lois types procurent un solide fondement pour la protection des données à caractère personnel et la facilitation des flux d'informations internationaux, visant à garantir la cohérence des pratiques de protection des données dans tous les États membres. Néanmoins, étant donné que les Lois types ont été conçues voici plus d'une décennie, elles contiennent de nombreuses lacunes et ont donc besoin d'être réactualisées (SADC, 2021).

2.2.2 CADRES RÉGLEMENTAIRES AU NIVEAU NATIONAL

Compte tenu de l'importance croissante de la protection des données, plusieurs pays africains ont commencé à élaborer des politiques et des stratégies visant à promouvoir le développement et l'utilisation des données. Avant 2016, seuls 16 pays africains disposaient de lois relatives à la protection des données. En 2021, 33 pays, soit 60 % du continent, avaient adopté de telles lois.[7] Toutefois, dans environ la moitié de ces juridictions, les lois sur la protection des données ne sont pas encore entrées en vigueur ou ne sont pas pleinement mises en œuvre (Greenleaf & Cottier, International and regional commitments in African data privacy laws: A comparative analysis, 2022).

D'une manière générale, la législation et les réglementations qui ont été élaborées sur l'ensemble du continent comprennent certains éléments communs, tels que les principes du traitement des données et les droits des personnes concernées. Cependant, il existe également des divergences entre les législations des différents pays. Par exemple, en ce qui concerne le champ d'application, certains pays peuvent appliquer les lois sur la protection des données uniquement au secteur privé ou au secteur public. Il peut également y avoir des divergences en ce qui concerne la définition des données à caractère personnel ou le traitement des flux transfrontaliers d'informations et ce qui constituerait une équivalence.

Selon une Analyse continentale sur le paysage de la protection des données et de la localisation en Afrique menée par la CUA dans le cadre de l'Initiative politique et réglementaire pour l'Afrique numérique (IPRA), l'objectif est d'évaluer les pays pour voir le niveau d'alignement et de convergence de leurs politiques, réglementations et législations nationales par rapport à 10 indicateurs/principes d'harmonisation, à savoir :

7 Il s'agit notamment du Cap-Vert (2001, modifiées en 2013), des Seychelles (2003), du Burkina Faso (2004, révisées en 2021), de Maurice (2004, révisées en 2017), de la Tunisie (2004, en cours de révision), du Sénégal (2008, en cours de révision), du Bénin (2009, révisées en 2017), du Maroc (2009, en cours de révision), de l'Angola (2011), du Gabon (2011), du Lesotho (2011), du Ghana (2012), de la Côte d'Ivoire (2013), du Mali (2013), de l'Afrique du Sud (2013), de Madagascar (2014), du Tchad (2015), de Malawi (2016), de la Guinée équatoriale (2016), de São Tomé-et-Principe (2016), de la Guinée (Conakry) (2016), de la Mauritanie (2017), du Niger (2017), de l'Algérie (2018), du Botswana (2018), du Nigeria (2019), de l'Ouganda (2019), du Kenya (2019), de la République du Congo (2019), du Togo (2019), de l'Égypte (2020), du Rwanda (2021) et du Zimbabwe (2002).

1. Droit à la vie privée et cadre juridique ;
2. Droits des individus en matière de la protection des données ;
3. Circulation transfrontalière des données à caractère personnel ;
4. Dispositions habilitantes concernant l'économie numérique ;
5. Application adéquate de la loi sur la protection des données ;
6. Garanties de sécurité suffisantes ;
7. Limites spécifiques à la confidentialité des informations ;
8. Coopération avec la société civile ;
9. Engagement multilatéral et bilatéral ;
10. Formation et développement des compétences.

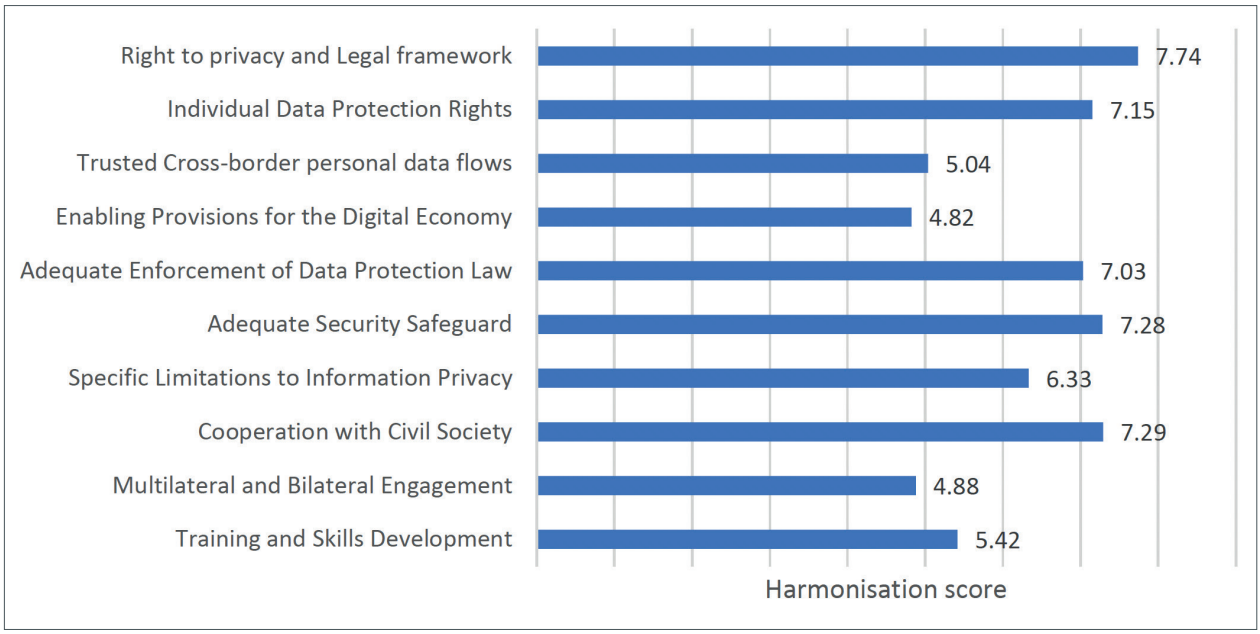
L'analyse comparative est menée une fois que les principes/indicateurs sont identifiés grâce à l'analyse du contenu des cadres régionaux et continentaux liés aux données, et qu'un indice d'harmonisation est créé à l'aide des principes d'harmonisation. L'analyse comparative permet de comparer les principes/indicateurs identifiés avec les pratiques juridiques du pays. Cette étape permet de vérifier si l'indicateur/les principes sont mis en œuvre dans le pays concerné. Par conséquent, dans le cadre de l'analyse, seuls les documents officiels, légaux et réglementaires sont consultés/utilisés à des fins de comparaison. L'analyse comprend sept étapes, à savoir : i) parcourir et préqualifier le document juridique, ii) identifier les sections pertinentes, iii) rechercher des mots-clés (mots-clés prédéterminés à partir des principes identifiés), iv) mettre en évidence les dispositions avec le mot-clé pertinent, v) comparer la disposition dans le document juridique avec le document principal/l'indicateur, vi) analyser et noter le degré d'harmonisation avec le document principal/l'indicateur comme base de la note, vii) procéder de la même façon pour le document principal/l'indicateur suivant.

La notation est utilisée comme technique pour fixer les valeurs d'une variable particulière selon que le pays en question a harmonisé ou non un aspect donné d'un principe où l'indicateur oscille sur une échelle entre zéro (0) et dix (10), où 0 indique un vide juridique/réglementaire, 5 une conformité partielle et 10 une conformité totale.

Alors qu'une évaluation et une analyse ont été menées au niveau national, où certains rapports nationaux, qui reflètent le degré d'harmonisation de chaque pays, démontrent différents niveaux dans l'adoption et la mise en œuvre des lois et règlements sur la protection des données et la localisation, une vue d'ensemble de l'état de la politique de protection des données, des législations et des règlements à travers les 33 pays participants en Afrique a été fournie. Comme le montre le point Figure 7 ci-dessous, globalement, beaucoup de travail a été accompli sur le droit à la vie privée et les cadres juridiques, les droits des individus en matière de la protection des données, les garanties de sécurité suffisantes et la coopération avec la société civile, de nombreux pays ayant mis en place des plates-formes pour le partage d'informations et la sensibilisation à la vie privée et à la protection des données. Toutefois, malgré ces bons résultats, certaines lacunes affectent les processus d'harmonisation au niveau continental. En revanche, les indicateurs dont les performances sont les plus faibles et qui nécessitent beaucoup plus d'interventions au niveau national et continental sont les suivants :

a. Circulation transfrontalière fiable des données ;
b. Dispositions habilitantes concernant l'économie numérique ;
c. Limites spécifiques à la confidentialité des informations ;
d. Engagement multilatéral et bilatéral ; et
e. Formation et développement des compétences.

Illustration 7. Niveau d'harmonisation des politiques et réglementations nationales en Afrique en matière de protection des données et de localisation



Source : CUA (2023)

Globalement, l'harmonisation des lois reste un défi malgré les progrès significatifs réalisés ces dernières années dans l'élaboration de politiques, de lois et de règlements sur l'ensemble du continent. Cela est dû à l'absence de cadre commun qui fournit une base pour la mise en œuvre et au manque de personnes qualifiées en matière de données possédant les compétences adéquates pour assurer une gouvernance des données et une création de valeur efficaces. Si la Convention de Malabo constitue un bon point de départ, son adoption a été lente, ce qui a nui à son envol et à sa mise en œuvre. Parmi les pays qui disposent d'une législation sur la protection des données, très peu l'ont complètement mise en œuvre. Afin de faciliter l'harmonisation de la circulation des données au niveau national et entre les pays pour soutenir le commerce numérique africain et l'économie fondée sur les données, les lois et les autorités des États membres doivent être renforcées et des programmes de formation et de développement des compétences à l'échelle du continent sont essentiels pour permettre aux pays de gérer eux-mêmes leurs données et de faciliter des transferts de données transfrontaliers sûrs et fiables.

En résumé, si l'élaboration de lois sur la protection des données dans de nombreuses juridictions représente une avancée importante, il est évident que ces lois sont élaborées de manière unilatérale. Sans une approche harmonisée et coordonnée, le continent héritera probablement de politiques et de stratégies fragmentées et diverses. Cela aura des conséquences néfastes sur la mise en œuvre effective de la ZLECAf. Lors de la rédaction du Protocole de la ZLECAf sur le commerce numérique, il est essentiel de prendre en compte les spécificités de la législation dans les différentes juridictions et de s'assurer que les États membres sont prêts à passer à un ensemble commun de normes et de pratiques afin de garantir l'homogénéité et la cohérence. En outre, comme le montre la section précédente, de nombreux développements ont été entrepris aux niveaux continental et régional. Ces éléments constitueraient des étapes importantes pour bien rédiger les dispositions relatives aux données dans le Protocole.

Lectures complémentaires

- Union africaine. (2020). La stratégie de transformation numérique pour l'Afrique (2020-2030).
- Union africaine. (2022). Cadre stratégique en matière des données de l'UA.
- OMC. (n.d.). Initiative conjointe sur le commerce électronique. De l'Organisation mondiale du commerce : *https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm*
- OCDE. (2013). Recommandation du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel. De *https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188*
- CNUCED (2021). Rapport sur l'économie numérique 2021 : Circulation transfrontalière des données et développement : Pour qui les données circulent. Conférence des Nations unies sur le commerce et le développement
- UNDG (2017). Note d'orientation des Objectifs de développement durable des Nations unies sur le Big Data pour la réalisation de l'Agenda 2030 : Confidentialité, éthique et protection des données. Groupe des Nations unies pour le développement.
- FEM (2020). Libre circulation des données en toute confiance (DFFT) : Vers une circulation ouverte et fiable des données. Forum économique mondial
- Burri, M. (2021). « Big Data and Global Trade Law ». Cambridge : Cambridge University Press.
- Gao, H. (18 janvier 2022). Souveraineté des données et accords commerciaux : Three digital kingdoms. Hinrich Foundation.

3. GUIDE DE RÉFÉRENCE POUR INTÉGRER LES DISPOSITIONS RELATIVES AUX DONNÉES DANS LE PROTOCOLE DE LA ZLECAF SUR LE COMMERCE NUMÉRIQUE

3.1 OBJECTIFS ET PORTÉE

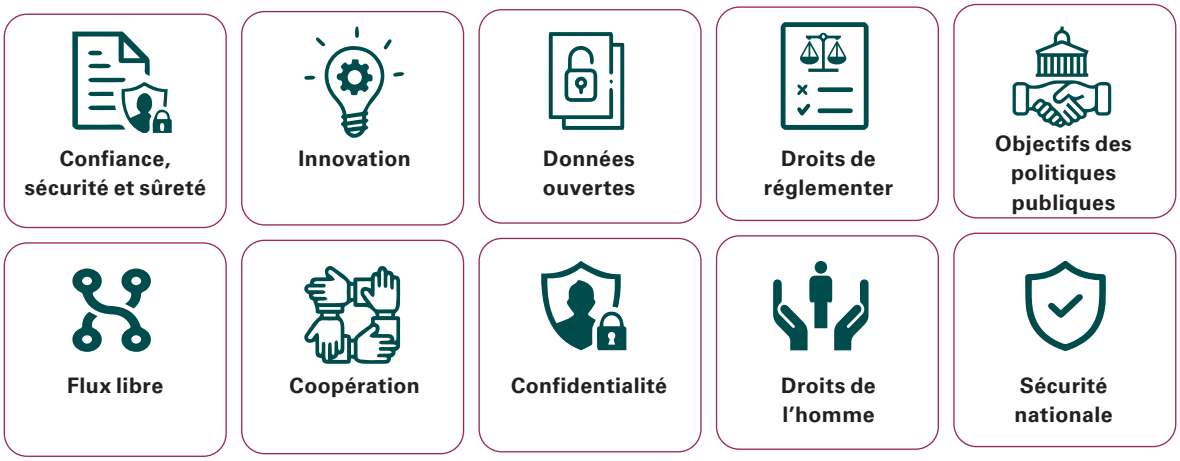
Les présentes lignes directrices au titre de l'intégration des dispositions relatives aux données dans les protocoles sur le commerce numérique sont en phase avec le Cadre stratégique en matière des données de l'UA, tel qu'approuvé par l'Union africaine en février 2022, définissant la vision qui amènera les États membres de l'Union africaine à développer leurs systèmes de données nationaux (African Union, 2022). Cela peut servir de base aux principes généraux orientant la gouvernance et l'utilisation des données. En ce qui concerne le rôle des données dans le commerce et l'économie numériques, l'objectif et la finalité peuvent être multiples : promouvoir l'innovation et la croissance économique ; fournir un environnement sûr et sécurisé pour renforcer la confiance ; préserver la marge de manœuvre des États dans la protection d'intérêts publics légitimes, tels que la sécurité nationale et les droits de l'homme ; ou équilibrer les avantages et les responsabilités des parties qui s'engagent dans l'économie numérique.

Il convient de souligner que les dispositions des ACR, y compris les dispositions relatives aux données, sont contraignantes pour les États membres des accords et qu'elles ne constituent donc que les engagements minimaux des parties. Cela correspond au principe du « droit de réglementer », selon lequel les dispositions des ACR ne servent que de règles générales minimales, tandis que les États ont le pouvoir de concevoir la spécificité de leurs réglementations nationales respectives pour l'application de ces règles.

Bien que les préambules ne soient généralement pas considérés comme ayant une signification juridique immédiate (Schenker, 2015) puisqu'ils ne précisent pas les obligations des Parties comme la plupart des clauses substantielles, les déclarations fournies dans la section préambule seront utilisées à des fins d'interprétation des dispositions conformément à l'article 31 de la Convention de Vienne sur le droit des traités de 1969.[8] Le préambule d'un traité définit, d'une manière générale, les buts, les considérations ou les motivations qui ont conduit les parties à conclure un traité (Mbengue, 2006). En d'autres termes, les préambules sont souvent associés à l'objet et à la finalité d'un traité. En tant que partie intégrante d'un traité, le texte du préambule est de plus en plus associé à un poids juridique et interprétatif substantiel, en particulier dans les contextes récents de l'OMC et des différends internationaux en matière d'investissement (Hulme, 2016). Cela incite fortement les négociateurs à examiner attentivement les implications que les préambules peuvent avoir lors de l'élaboration des textes d'ouverture des traités.

8 L'article 31 (Règle générale d'interprétation) de la Convention de Vienne de 1969 stipule que :
1. Un traité doit être interprété de bonne foi suivant le sens ordinaire à attribuer à ses termes dans leur contexte et à la lumière de son objet et de sa finalité.
2. Le contexte aux fins de l'interprétation d'un traité comprend, outre le texte, y compris le préambule et les annexes : a) tout accord ayant rapport au traité qui a été conclu entre toutes les parties à l'occasion de la conclusion du traité ; b) tout instrument établi par une ou plusieurs parties à l'occasion de la conclusion du traité et accepté par les autres parties en tant qu'instrument ayant rapport au traité. [...]

Illustration 8. Quelques considérations clés concernant les dispositions relatives aux données dans les ALE



Sur la base de la formulation de la vision du Cadre stratégique en matière des données de l'UA, le texte suivant pourrait servir d'exemple pour les déclarations de préambule relatives aux données de l'Accord ZLECAf sur le commerce numérique afin de soutenir l'utilisation responsable, sûre et équitable des données :

[Les parties au présent Accord, décidant ce qui suit :][9]

- Reconnaître le potentiel de transformation des données pour autonomiser les pays africains, améliorer la vie des gens, préserver les intérêts collectifs, protéger les droits numériques et favoriser un développement socio-économique équitable ;
- Reconnaître la nécessité **de systèmes de données de confiance**, sûrs et sécurisés, intégrés sur la base de normes et de pratiques communes ;
- Reconnaître la nécessité d'un environnement favorable qui stimule **l'innovation** et l'esprit d'entreprise afin de favoriser le développement d'économies fondées sur la valeur des données ;
- Reconnaître la nécessité de **données ouvertes**, de normes d'interopérabilité et d'initiatives de partage des données afin d'exploiter le potentiel des données pour stimuler le développement et assurer une meilleure répartition des avantages de l'économie fondée sur les données ;
- Reconnaître la nécessité de garantir la souveraineté des États membres et leur capacité à fixer des priorités législatives et réglementaires et **réglementer** le paysage des données en constante évolution, ainsi qu'à accroître l'utilisation productive et innovante des données pour fournir des solutions et créer de nouvelles opportunités tout en atténuant les risques dans l'économie numérique ;
- Reconnaître la nécessité d'une **approche équilibrée** pour faciliter la libre circulation des données à travers les frontières tout en assurant une répartition équitable des avantages et en tenant compte des risques liés au bien-être public, aux droits de l'homme, à la sécurité nationale et à d'autres objectifs légitimes de politique publique ;

9 Cette liste d'exemples de préambules n'est pas exhaustive et ne couvre pas les objectifs plus généraux du chapitre sur le commerce numérique.

- Réaffirmer l'importance de promouvoir la responsabilité sociale des entreprises, l'identité et la diversité culturelles, la protection et la préservation de l'environnement, l'égalité des genres, les droits des populations autochtones, les droits du travail, le commerce inclusif, le développement durable et les connaissances traditionnelles, ainsi que l'importance de préserver le droit de réglementer des États dans l'intérêt public ;
- Reconnaître la nécessité de faciliter la circulation transfrontalière des données et d'accroître les opportunités commerciales tout en garantissant un niveau adéquat de protection des **données à caractère personnel et de la confidentialité ;**
- Reconnaître la nécessité pour les États membres de **coopérer** sur les questions de gouvernance des données afin d'atteindre des objectifs communs liés au développement durable de leurs économies et de leurs sociétés.

Ces déclarations présentent la vision et les objectifs du Protocole sur le commerce numérique. En règle générale, elles ne sont pas particulièrement contraignantes et ne prévoient aucun engagement en termes de restriction ou de facilitation des flux de données. Le préambule est une déclaration d'intention sur la manière dont les parties souhaitent réglementer et faciliter certains aspects du marché des données et souligne l'alignement des parties sur certains principes fondamentaux.

3.2 CONSIDÉRATIONS DES DISPOSITIONS ESSENTIELLES

Cette section présente des considérations sur les dispositions essentielles, y compris, le cas échéant, la nécessité d'avoir de telles dispositions dans le contexte africain ; les implications pour la réglementation, la compétitivité et l'accès au marché ; les éventuels problèmes de mise en œuvre et les options pour les différents types de négociations (en termes de domaines d'intérêt).

Cette section se concentre sur neuf dispositions qui sont étroitement liées à la gouvernance des données ou qui ont un impact sur l'utilisation responsable, sûre et équitable des données (voir la liste ci-dessous). Les règles liées au cadre stratégique en matière des données peuvent également figurer dans les protocoles relatifs à la concurrence et à la propriété intellectuelle, mais ceux-ci n'entrent pas dans le champ d'application du présent guide politique et ne sont, donc, pas inclus.

En guise d'approche générale, sur la base de la taxonomie et de l'analyse du texte de différents accords, cette section propose un certain nombre d'options pour différentes dispositions relatives aux données.[10] Pour faciliter la navigation parmi les options, les différents niveaux d'engagement sont indiqués par des combinaisons de verbes et de verbes modaux entre crochets ([...]) : de simples aspirations (comme indiqué par l'utilisation de « Les Parties reconnaissent », « s'efforcent de », « veillent à », etc.) à des engagements plus fortement contraignants (par l'utilisation de « doivent », « adoptent », « ne manquent pas de », etc.) (Baker, 2021). Des terminologies alternatives sont également fournies entre crochets ([...]) pour indiquer les options possibles. Le numéro de l'option est indiqué dans chacune des options possibles s'excluant mutuellement pour faciliter la lecture des négociateurs. Certaines

10 Il est à noter que, dans le présent guide, les dispositions de type (ou de sous-type) sont séparées en fonction de leur contenu / question réglementée ; par conséquent, un article peut comprendre une ou plusieurs dispositions (ou clauses). Les dispositions ne s'excluent pas nécessairement les unes les autres et plusieurs options non contradictoires peuvent être sélectionnées par les négociateurs pour être incluses dans le texte de négociation.

dispositions, telles que celles relatives à la coopération ou à l'innovation en matière de données, sont généralement similaires dans la plupart des accords, car elles n'imposent pas d'obligations contraignantes aux Parties. Par conséquent, une seule option (avec des choix de mots potentiellement différents) est fournie pour chacun de ces types de dispositions.

3.2.1. PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL / CONFIDENTIALITÉ DES DONNÉES

L'inclusion de mesures de protection des données à caractère personnel dans les accords commerciaux a été motivée par des préoccupations relatives à la vie privée des individus ou à la sécurité nationale (Banga, Macleod, & Mendez-Parra, 2021). Alors que la résistance à l'inclusion de la protection des données persiste par crainte de porter atteinte à la confidentialité (Greenleaf, 2018), les dispositions relatives aux questions de données récemment approuvées dans les négociations commerciales préférentielles peuvent offrir des possibilités d'équilibrer les objectifs contradictoires de la protection des données par rapport au protectionnisme (Burri, 2017), ainsi que d'élaborer une approche harmonisée de la protection des données dans l'ensemble des domaines. Cela est d'autant plus important dans le contexte de l'Afrique et des négociations de l'Accord ZLECAf sur le commerce numérique, car seuls 33 pays africains (soit 61 % de l'ensemble des États membres de l'UA) disposent d'une législation en vigueur sur la protection des données et de la confidentialité.

Selon la base de données TAPED, quatre-vingt-un des 370 ACR conclus au cours de la période 2000-2022 comprennent des dispositions sur la « protection des données » avec différents niveaux d4engagements contraignants (Burri, Callo-Müller, & Kugler, 2022). Si les dispositions des ACR relatives à la protection des données n'imposent pas les droits spécifiques des personnes concernées (comme les lois nationales), elles exigent souvent que les pays mettent en place un cadre juridique ou une mesure pour garantir la protection des informations personnelles (voir détails ci-dessous).

Outre les dispositions les plus courantes obligeant les Parties à disposer ou à maintenir un cadre juridique national sur la protection des données, de nombreux ACR prévoient également que, lors de l'élaboration de normes de protection des données à caractère personnel en ligne, chaque partie prenne en compte les normes internationales existantes ou les lignes directrices des organisations internationales compétentes – telles que le Cadre de protection de la vie privée de l'APEC ou les Lignes directrices de l'OCDE sur les flux transfrontières de données à caractère personnel (2013). Certains accords précisent même les principes de protection des données à caractère personnel, notamment les principes de limitation de la finalité, de qualité et de proportionnalité des données, de transparence, de sécurité, de droit d'accès, de rectification et d'opposition, de restriction des transferts ultérieurs et de protection des données sensibles, ainsi que des dispositions relatives aux mécanismes d'application, à la cohérence avec les engagements internationaux et à la coopération entre les parties afin d'assurer un niveau adéquat de protection des données à caractère personnel.[11]

De nombreux ACR contenant des dispositions relatives à la protection des données reconnaissent également les différentes approches juridiques des Parties en matière de protection des informations personnelles, et encouragent, donc, les Parties à créer des mécanismes visant à promouvoir la compatibilité entre ces différents cadres réglementaires. Ces mécanismes peuvent inclure la reconnaissance des résultats réglementaires, qu'ils soient

11 Article 199-200, APE CARIFORUM-CE

accordés de manière autonome (comme la décision d'adéquation de l'UE), d'un commun accord (comme le bouclier de protection de la vie privée UE-États-Unis, qui a été déclaré invalide par la Cour de justice de l'Union européenne le 16 juillet 2020), ou dans des cadres internationaux plus larges (comme les Lignes directrices de l'OCDE sur la protection de la vie privée ou les Règles de confidentialité transfrontalières de l'APEC).

Étant donné que les pays peuvent se trouver à différents stades de développement du cadre juridique national en matière de protection des données, des activités de coopération ont également été incorporées dans les ACR afin d'améliorer le niveau de protection de la vie privée dans les communications électroniques tout en évitant les obstacles au commerce. Ces dispositions peuvent inclure le partage d'informations et d'expériences sur les réglementations, les lois et les programmes relatifs à la protection des données ; des activités de recherche et de formation ; l'établissement de programmes et de projets communs ; le maintien d'un dialogue ; l'organisation de consultations sur les questions de protection des données, etc (Burri, 2021). Il est également important que les parties à l'accord s'efforcent de reconnaître l'adéquation des réglementations entre elles, ce qui est encouragé dans le CPTPP (Baker & Le, 2022).

Sur la base de ces considérations, les options suivantes sont proposées pour les dispositions relatives à la Protection des données à caractère personnel. Dans le contexte africain, la Convention de Malabo représente une étape importante pour l'harmonisation du cadre réglementaire du continent en matière de Cybersécurité et de Protection des données à caractère personnel. Une disposition type est donc ajoutée pour encourager les États membres de l'UA à accélérer le processus de ratification.

(I) OBJECTIFS

Réaffirmation des avantages de la protection des données à caractère personnel : Les États parties[12] reconnaissent les avantages économiques et sociaux de la protection des [*informations/données*] à caractère personnel des participants à [*l'économie numérique / au commerce numérique / au commerce électronique*] et l'importance de cette protection pour renforcer la confiance dans [*l'économie numérique / le commerce numérique / le commerce électronique*].[13]

Reconnaître le droit à la vie privée : Les États parties reconnaissent que la protection des [*informations/données*] à caractère personnel et de la vie privée est un droit fondamental et que des normes strictes à cet égard contribuent à la confiance dans l'économie numérique et au développement du commerce.

Mettre l'accent sur la proportionnalité des mesures de protection des données : Les États parties reconnaissent qu'il est important de veiller au respect des mesures de protection des données à caractère personnel et de s'assurer que toute restriction aux flux transfrontaliers de données à caractère personnel est nécessaire et proportionnée aux risques encourus. [14]

12 La plupart des ACR utilisent les termes « Parties » ou « Membres » pour désigner les signataires. La ZLECA utilise le terme « État partie » pour désigner un État membre de l'Union africaine qui a ratifié l'Accord ou y a adhéré et pour lequel l'Accord est en vigueur. Par conséquent, ce guide utilise également le terme « État partie » (ou « États parties » au pluriel) par souci de cohérence.

13 Sur la base de l'article 14.8.1 du CPTPP ; article 4.2.1 de l'APEN.

14 Paragraphe 3, section C.2.1, projet de texte de négociation de l'OMC sur le commerce électronique.

(II) RÉGLEMENTATIONS NATIONALES

[Option 1] Réglementations nationales visant à promouvoir le commerce numérique/ électronique : Chaque État partie [*peut/doit*] adopter [*et/ou*] maintenir [*un cadre / des mesures juridiques*] qui prévoit la protection des [*informations/données*] à caractère personnel des utilisateurs du commerce électronique et des échanges numériques.[15]

[Option 2] Les réglementations nationales pour assurer la protection de la vie privée : Les États parties [*peuvent/doivent*] adopter [*et/ou*] maintenir [*un cadre juridique / des mesures*] qui garantissent la protection des [*informations/données*] à caractère personnel, y compris le transfert et le traitement transfrontaliers des [*informations/données*] et les conditions et exigences y afférentes, afin de promouvoir les valeurs fondamentales que sont le respect de la vie privée et la protection des [informations/données] à caractère personnel. [16]

(III) CONSIDÉRATIONS PARTICULIÈRES POUR LES ÉTATS PARTIES[17] À UN STADE PRÉCOCE DE L'ÉLABORATION DES SYSTÈMES NATIONAUX DE DONNÉES

[Option 1] Autoriser l'État partie à élaborer un cadre national à son propre rythme : [*Nom de l'État partie*] n'est pas tenu d'appliquer le présent Article avant la date à laquelle ladite Partie met en œuvre son cadre juridique qui prévoit la protection des données à caractère personnel des utilisateurs du commerce électronique. Il est entendu qu'un État partie peut se conformer à l'obligation énoncée dans le présent Article en adoptant ou en maintenant des mesures telles que des lois générales sur la protection de la vie privée, des informations personnelles ou des données à caractère personnel, des lois sectorielles sur la protection de la vie privée, ou des lois qui prévoient l'application d'engagements volontaires pris par les entreprises en matière de protection de la vie privée.[18]

[Option 2] Prévoir une période transitoire spécifique à la demande de l'État partie : [*Nom de l'État partie*] est tenu d'appliquer le présent Article au plus tard le [*indiquer le nombre d'années de transition*] suivant la date d'entrée en vigueur du présent Accord pour ladite Partie. Nonobstant [*référence à une clause spécifique*], [*Nom de l'État partie*] peut demander une prolongation de [indiquer le nombre d'années de transition supplémentaires] pour mettre pleinement en œuvre les engagements pris au titre de [*référence à une clause spécifique*] en adressant une demande écrite au [*indiquer le comité spécifique*] au plus tard six mois avant l'expiration de la période de [*indiquer le nombre d'années de transition initiales*] prévue dans le présent paragraphe.

(IV) ADOPTION DE LIGNES DIRECTRICES INTERNATIONALES

[Option 1] Encouragement général : Dans l'élaboration de son [*cadre / ses mesures juridiques*] pour la protection des [*informations/données*] à caractère personnel, chaque État partie tient compte des principes et lignes directrices des organismes internationaux compétents.[19]

---

15 Sur la base de la première phrase de l'article 14.8.2 du CPTPP ; l'article 12.8 du RCEP ; la première phrase de l'article 4.2 de l'APEN.

16 Paragraphe 4, section C.2.1, projet de texte de négociation de l'OMC sur le commerce électronique.

17 Ces exemples de clauses sont fournis dans le cadre de la disposition relative à la Protection des données à caractère personnel, mais les États parties peuvent également envisager d'insérer un libellé similaire dans d'autres dispositions en fonction des besoins et de l'accord entre les États parties.

18 Sur la base des notes de bas de page 5 et 6 du CPTPP.

19 Sur la base de la deuxième phrase de l'article 14.8.2 du CPTPP et de la deuxième phrase de l'article 4.2 de l'APEN.

[Option 2] Indiquer les lignes directrices internationales spécifiques : Dans l'élaboration de son [*cadre / mesures juridiques*] pour la protection des [*informations/données*] à caractère personnel, chaque État partie [*devra/peut/doit*] tenir compte des normes, principes, lignes directrices et critères internationaux des organisations ou organes internationaux compétents, tels que la Recommandation du Conseil de l'OCDE concernant les Lignes directrices régissant la protection de la vie privée et la circulation transfrontalière de données à caractère personnel (2013).[20]

(V) PRINCIPES CLÉS

Mettre l'accent sur le principe du consentement des utilisateurs : Les États parties veillent à obtenir le consentement directement exprimé par la personne concernée pour le transfert et le traitement transfrontaliers de ses données à caractère personnel.[21]

Énumération des principes clés pour le cadre juridique national : Les États parties reconnaissent que les principes qui sous-tendent un cadre juridique solide pour la protection des informations personnelles devront inclure la limitation de la collecte, le choix, la qualité des données, la spécification des finalités, la limitation de l'utilisation, les garanties de sécurité, la transparence, la participation individuelle et l'obligation de rendre des comptes.[22]

(VI) ENGAGEMENT À RATIFIER LA CONVENTION DE MALABO

Les États parties déploieront des efforts continus et soutenus en vue de ratifier la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel de 2014 (la Convention de Malabo). Les États parties [*s'engagent/s'efforcent*] de respecter, de promouvoir et de mettre en œuvre, dans leurs lois et pratiques, les principes énoncés dans la Convention de Malabo.

(VII) NON-DISCRIMINATION

Règle générale de non-discrimination concernant les données à caractère personnel des utilisateurs du commerce électronique : Chaque État partie [*s'efforce de/doit*] adopter des pratiques non discriminatoires pour protéger les utilisateurs du commerce électronique contre les violations de la protection des données à caractère personnel survenant dans sa juridiction.[23]

Non-discrimination en mettant l'accent sur l'information des consommateurs et des patients médicaux : Chaque État partie [*s'efforce de/doit*] adopter des pratiques non discriminatoires pour protéger les citoyens, les consommateurs et les patients médicaux contre les violations de la protection des données à caractère personnel survenant dans sa juridiction.[24]

20 Sur la base du paragraphe 5, section C.2.1, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.
21 Paragraphe 8, section C.2.1, projet de texte de négociation de l'OMC sur le commerce électronique.
22 Sur la base de l'article 19.8.3 de l'ACEUM ; de l'article 4.2.3 de l'APEN.
23 Sur la base de l'article 4.4 de l'APEN ; l'article 14.8.3 du CPTPP ; l'article 19.8.4 de l'ACEUM ; le paragraphe 7, section C.2.1, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.
24 Paragraphe 7, section C.2.1, projet de texte de négociation de l'OMC sur le commerce électronique.

(VIII) PUBLICATION D'INFORMATIONS

Chaque État partie [*devra/doit*] publier des informations sur la protection des informations personnelles qu'il fournit aux utilisateurs du commerce électronique, y compris sur la manière dont il le fait : a) les particuliers peuvent exercer des recours ; b) les entreprises peuvent se conformer aux exigences légales. [25]

(IX) PROMOUVOIR LA COMPATIBILITÉ DES RÉGIMES

Mécanismes visant à promouvoir la compatibilité et/ou la reconnaissance mutuelle : Reconnaissant que les États parties peuvent adopter des approches juridiques différentes en matière de protection des informations à caractère personnel, chaque État partie [poursuit/encourage] l'élaboration de mécanismes visant à promouvoir la compatibilité [et/ou] l'interopérabilité entre leurs différents régimes de protection des informations à caractère personnel.[26] Ces mécanismes peuvent comprendre : a) la reconnaissance des résultats réglementaires, qu'ils soient accordés de manière autonome ou d'un commun accord ; b) des cadres internationaux plus larges;[27] c) lorsque cela est possible, la reconnaissance appropriée d'une protection comparable accordée par les cadres nationaux de certification ou de marque de confiance de leurs cadres juridiques respectifs ; ou d) d'autres voies de transfert d'informations à caractère personnel entre les États parties.[28]

Échange d'informations : Les États parties [s'efforcent de/doivent] échanger des informations sur les mécanismes appliqués dans leurs juridictions et étudier les moyens d'étendre ces mécanismes ou d'autres dispositions appropriées afin de promouvoir la compatibilité entre eux.[29]

3.2.2. CIRCULATION TRANSFRONTALIÈRE DES DONNÉES

L'importance croissante des données dans l'économie a donné lieu à des discussions sur les règles régissant la circulation transfrontalière des données. Les restrictions au transfert transfrontalier de données dépendent de l'approche de la souveraineté en matière de données adoptée par un pays. Les limites imposées au transfert transfrontalier de données pourraient entraîner la perte d'opportunités commerciales et réduire la capacité d'une organisation à commercer à l'échelle internationale. L'approche générale du transfert de données exige un niveau de protection adéquat dans le pays destinataire. Par exemple, la Convention de Malabo, tout en garantissant la libre circulation de l'information, exige que « *Le responsable du traitement des données ne transfère pas de données à caractère personnel à un État non membre de l'Union africaine à moins que ledit État n'assure un niveau adéquat de protection de la vie privée, des libertés et des droits fondamentaux des personnes, dont les données sont traitées ou susceptibles de l'être.* »[30] Dans ce contexte, il est essentiel d'établir le principe de base de la protection des données qui prévoit une synchronisation ou une similitude avec les réglementations d'autres juridictions afin de jeter les bases d'un échange fiable de données, y compris de données à caractère personnel.

25 Sur la base de l'article 4.5 de l'APEN ; l'article 14.8.4 du CPTPP ; l'article 19.8.5 de l'ACEUM ; l'article 12.8.3 du RECP ; du paragraphe 9, section C.2.1, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.
26 Sur la base de la première phrase de l'article 19.8.6 de l'ACEUM.
27 Sur la base des première et deuxième phrases de l'article 14.8.5 du CPTPP.
28 Sur la base de l'article 4.6 de l'APEN ; paragraphes 10 et 11, section C.2.1, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.
29 Sur la base de l'article 4.7de l'APEN ; deuxième phrase, article 19.8.6 de l'ACEUM.
30 Article 14.6 a), Convention de Malabo.

Le Cadre stratégique en matière des données de l'UA encourage les États membres à tirer parti des économies d'échelle de l'infrastructure numérique offerte par les services en nuage et d'autres nouvelles technologies pour la création de valeur des données pour les secteurs privé et public (African Union, 2022). Cela impliquerait la nécessité d'autoriser la libre circulation transfrontalière des données sur le continent et au-delà, sous réserve de conditions et de normes visant à garantir la sécurité des données. En outre, la libre circulation intracontinentale des données sera un élément essentiel pour la création du marché commun africain et en particulier pour la réalisation de la vision d'un Marché numérique unique africain tel que prévu dans la Stratégie de transformation numérique pour l'Afrique (2020-2030) (African Union, 2020).

Les références à la circulation des données sont apparues dans les ACR dès les années 2000. Dans le cadre de l'ALE entre la Jordanie et les États-Unis, la Déclaration conjointe sur le commerce électronique souligne la « nécessité de poursuivre la libre circulation de l'information » (Burri, 2021). Depuis lors, un nombre croissant d'ACR a intégré des dispositions plus contraignantes pour faciliter la circulation transfrontalière des données. Toutefois, les cadres juridiques actuels sur la circulation transfrontalière des données présentent une grande diversité (UNCTAD, 2023). En conséquence, le champ d'application de la circulation transfrontalière des données a été moins solide que celui de la protection des données, d'où la nécessité de concilier les approches différenciées du transfert transfrontalier de données, y compris de données à caractère personnel.

D'une manière générale, on trouve trois types de dispositions relatives à la circulation transfrontalière des données dans les ACR existants, y compris ceux dont le champ d'application est le plus étendu, tels que l'APEN ou le DEA entre le Royaume-Uni et Singapour. Il s'agit notamment de dispositions invoquant le droit de réglementer, l'engagement de permettre le transfert transfrontalier d'informations par voie électronique et le traitement non discriminatoire. [31] Les conditions spécifiques du transfert transfrontalier doivent toutefois être réglementées au niveau national. Cela correspond probablement à l'accent mis par les Parties sur le droit de réglementer, mais nécessite également un travail de collaboration aux niveaux bilatéral et régional, en particulier dans le contexte de l'Afrique, afin de garantir à la fois la libre circulation des données et leur sécurité.

Sur la base des pratiques actuelles, le tableau ci-dessous présente les différentes options pour ces types de circulation transfrontalière des données prévus par l'Accord ZLECAf sur le commerce numérique.

(I) OBJECTIFS

Équilibre des droits : Les États parties reconnaissent l'importance de la libre circulation de l'information sur Internet, tout en convenant qu'elle ne doit pas porter atteinte aux droits d'autres personnes, entités ou entreprises, y compris les droits de propriété intellectuelle.

31 La règle de non-discrimination met également l'accent sur le pouvoir d'une Partie de réglementer pour servir des objectifs de politique publique et, par conséquent, dans ce guide, nous incluons ce type de disposition dans la même cohorte du « droit de réglementer ».

(II) RECONNAISSANCE DES DROITS DE RÉGLEMENTER

Droit générique de réglementer : Les États parties reconnaissent que chaque État partie peut avoir ses propres exigences réglementaires concernant le transfert d'informations par voie électronique.[32]

Droit de réglementer en fonction des intérêts essentiels de sécurité : Aucune disposition du présent Article n'empêche un État partie d'adopter ou de maintenir toute mesure qu'il juge nécessaire à la protection des intérêts essentiels de sa sécurité.[33]

Droit de réglementer sans discrimination ni entrave au commerce : Aucune disposition du présent Article n'empêche un État partie d'adopter ou de maintenir une mesure incompatible avec [une exigence relative à l'autorisation des transferts transfrontaliers d'informations par voie électronique] qu'il juge nécessaire pour atteindre un objectif légitime de politique générale, à condition que la mesure : a) ne soit pas appliquée d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable ou une restriction déguisée au commerce;[34] et b) n'impose pas de restrictions aux transferts d'informations plus importantes que celles qui sont nécessaires pour atteindre l'objectif. [35]

(III) GOUVERNANCE DE LA CIRCULATION TRANSFRONTALIÈRE DES DONNÉES

[Option 1] Obligation de moyens : Les États parties s'efforcent de soutenir la circulation transfrontalière des données en toute confiance grâce à des contrats types de protection des données et à l'utilisation de technologies émergentes. Les deux parties étudieront également la possibilité de collaborer sur l'utilisation de technologies visant à renforcer la protection de la vie privée.[36]

[Option 2] Flux libre sans condition : Aucun État partie ne doit [*interdire/restreindre/prévenir*] le transfert transfrontalier d'informations [*nul / incluant des informations à caractère personnel*] par voie électronique lorsque cette activité est destinée à la conduite des affaires d'une personne visée.[37]

[Option 3] Flux libre sans exigences de localisation : Les États parties s'engagent à assurer la circulation transfrontalière des données afin de faciliter les échanges dans l'économie numérique. À cette fin, la circulation transfrontalière des données ne doit pas être limitée par :[38]

---

32 Sur la base de l'article 4.3.1 de l'APEN ; l'article 14.11.1 du CPTPP ; l'article 12.15.1 du RCEP ; paragraphe 4, section B.2.1, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.

33 Sur la base de l'article 12.15.3 b) du RCEP ; paragraphe 6, section B.2.1, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.

34 Sur la base de l'article 12.15.3 a) du RCEP.

35 Sur la base de l'article 4.3.3 de l'APEN ; l'article 19.11.2 de l'ACEUM ; l'article 14.11.3 du CPTPP ; paragraphe 6, section B.2.1, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.

36 Sur la base du paragraphe 26, section 4, partenariat numérique UE-Singapour.

37 Sur la base de l'article 19.11.1 de l'ACEUM ; article 12.15.2 du RCEP ; paragraphe 5, section B.2.1, projet de texte de négociation des négociations de l'OMC sur le commerce électronique. L'article 4.3.2 de l'APEN et l'article 14.11.2 du CPTPP expriment la même notion dans une clause affirmative plutôt que négative : « Chaque partie autorise le transfert transfrontalier d'informations par voie électronique, y compris d'informations à caractère personnel, lorsque cette activité est destinée à la conduite des affaires d'une personne visée. »

38 Le paragraphe 5, section B.2.1, projet de texte de négociation de l'OMC sur le commerce électronique ; article 201, accord de libre-échange UE-Royaume-Uni.

a. exiger l'utilisation d'installations informatiques ou d'éléments de réseau sur le territoire de l'État partie pour le traitement, y compris en imposant l'utilisation d'installations informatiques ou d'éléments de réseau certifiés ou agréés sur le territoire de l'État partie ;
b. exiger la localisation des données sur le territoire de l'État partie en vue de leur stockage ou de leur traitement ;
c. interdire le stockage ou le traitement sur le territoire d'autres États parties ;
d. subordonner le transfert transfrontalier de données à l'utilisation d'installations informatiques ou d'éléments de réseau sur le territoire de l'État partie ou à des exigences de localisation sur le territoire de l'État partie.

3.2.3. LOCALISATION DES DONNÉES

Tout comme le transfert transfrontalier de données, la localisation des données, souvent appelée « implantation des installations informatiques », est souvent discutée dans le cadre de la souveraineté des données. La localisation des données implique des obstacles législatifs à la circulation des données, par exemple par le biais d'exigences obligatoires de stockage local des données (Cory, 2017). La localisation des données est motivée non seulement par la nécessité de protéger les personnes concernées, mais aussi de soutenir les politiques publiques et les réglementations nationales, en particulier dans des secteurs critiques tels que la fiscalité, la comptabilité, la finance ou les télécommunications.

D'une manière générale, les règles de localisation des données imposent la conservation des données ou une copie de celles-ci sur le territoire d'un pays. Les règles strictes de localisation des données exigent le stockage de toutes les données localement, et pas seulement une copie. Les règles de localisation des données sont souvent destinées à prévenir la cybercriminalité (comme le vol d'identité), à promouvoir les économies locales (par la création d'emplois) et à répondre aux préoccupations croissantes en matière de respect de la vie privée (McKinsey, 2022). Toutefois, lorsque les infrastructures de données locales ne sont pas suffisamment sûres, elles peuvent devenir vulnérables aux menaces de sécurité, telles que les cyberattaques et la surveillance étrangère. En outre, les exigences relatives aux copies des données peuvent imposer des obligations financières excessives aux entreprises. Certains pays africains sont confrontés à d'importantes contraintes de capacité technologique et, par conséquent, les exigences en matière de localisation des données pourraient en fait peser sur la capacité nationale de l'infrastructure numérique actuelle (telle que les centres de données nationaux) (African Union, 2022). C'est pourquoi il est essentiel que les États membres de l'UA évaluent l'application de la localisation des données sur une base coût-bénéfice, en intégrant la valeur publique, afin de faciliter l'innovation technologique tout en ne surchargeant pas la capacité de l'infrastructure nationale.

La première règle de localisation des données a été incluse dans l'accord de libre-échange entre le Japon et la Mongolie en 2015. Depuis lors, un nombre croissant d'accords commerciaux ont intégré cette règle dans leur chapitre sur le commerce électronique. Toutefois, à l'instar des règles relatives au transfert transfrontalier de données, le champ d'application actuel des règles de localisation des données dans le cadre des ACR est également limité par rapport à celui de la protection des données, d'où la nécessité de concilier les approches différenciées et l'accent mis sur la souveraineté des pays en matière de données.

D'une manière générale, on trouve trois types de dispositions sur la localisation des données dans les ACR existants, y compris ceux dont le champ d'application est le plus étendu, tels que l'APEN ou le DEA entre le Royaume-Uni et Singapour. Il s'agit notamment de dispositions invoquant le droit de réglementer, l'interdiction d'utiliser les exigences en matière de

localisation des données comme condition pour exercer une activité sur le territoire d'un pays, et le traitement non discriminatoire[39]. Comme pour les transferts transfrontaliers, les conditions spécifiques relatives à l'implantation obligatoire des installations informatiques doivent être réglementées au niveau national. Les services financiers ont une exigence distincte en matière de transfert de données, en vertu de laquelle certaines restrictions sur la circulation des données peuvent s'appliquer pour la protection de la vie privée ou la confidentialité des dossiers individuels, ou pour des raisons prudentielles. C'est pourquoi des options pour ce type de disposition sont également proposées ci-dessous.

(I) RECONNAISSANCE DES DROITS DE RÉGLEMENTER

Droit générique de réglementer : Les États parties reconnaissent que chaque État partie peut avoir ses propres [exigences/mesures réglementaires] concernant l'utilisation ou l'implantation des installations informatiques, y compris des [*exigences / mesures réglementaires*] visant à garantir la sécurité et la confidentialité des communications.[40]

Droit de réglementer en fonction des intérêts essentiels de sécurité : Aucune disposition du présent Article n'empêche un État partie d'adopter ou de maintenir toute mesure qu'il juge nécessaire à la protection des intérêts essentiels de sa sécurité.[41]

Droit de réglementer sans discrimination ni entrave au commerce : Aucune disposition du présent Article n'empêche un État partie d'adopter ou de maintenir des mesures incompatibles avec [l'interdiction de la localisation des données sur le territoire d'un État partie] qu'il juge nécessaires pour atteindre un objectif légitime de politique publique, à condition que la mesure : a) n'est pas appliquée d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable ou une restriction déguisée au commerce ;[42] et b) n'impose pas de restrictions à l'utilisation ou à l'implantation des installations informatiques plus strictes que celles qui sont [nécessaires/exigées] pour atteindre l'objectif.[43]

(II) INTERDICTION DE LOCALISATION DES DONNÉES

Aucun État partie n'exige d'une personne visée qu'elle utilise ou installe des moyens informatiques sur le territoire de cet État partie comme condition à la conduite d'activités sur ce territoire.[44]

---

39 La règle de non-discrimination met également l'accent sur le pouvoir d'une Partie de réglementer pour servir des objectifs de politique publique et, par conséquent, dans ce guide, nous incluons ce type de disposition dans la même cohorte du « droit de réglementer ».

40 Sur la base de l'article 4.4.1 de l'APEN ; l'article 12.14.1 du RCEP ; l'article 14.13.1 du CPTPP ; paragraphe 4, section B.2.2, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.

41 Sur la base de l'article 12.14.3 b) du RCEP ; paragraphe 7, section B.2.2, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.

42 Sur la base de l'article 12.14.3 a) du RCEP.

43 Sur la base de l'article 4.4.3 de l'APEN ; article 14.13.3 du CPTPP ; paragraphe 6, section B.2.2, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.

44 Sur la base de l'article 4.4.2 de l'APEN ; l'article 19.12 de l'ACEUM ; l'article 14.13.2 du CPTPP ; l'article 12.14.2 du RCEP ; paragraphe 5, section B.2.2, projet de texte de négociation des négociations de l'OMC sur le commerce électronique.

(III) IMPLANTATION DES INSTALLATIONS INFORMATIQUES POUR LE FOURNISSEUR DE SERVICES FINANCIERS COUVERT

[Option 1] Reconnaître la nécessité de l'accès à l'information pour la réglementation et la supervision financières : Les États parties reconnaissent que l'accès immédiat, direct, complet et permanent des autorités de régulation financière d'un État partie aux informations des fournisseurs de services financiers couverts, y compris les informations relatives aux transactions et opérations de ces personnes, est essentiel pour la régulation et la supervision financières, et reconnaissent la nécessité d'éliminer toute limitation potentielle de cet accès. [45]

[Option 2] Pas d'exigence de localisation des données sous réserve de conditions : Aucun État partie n'exige d'un fournisseur de services financiers couvert qu'il utilise ou implante des installations informatiques de services financiers sur le territoire de l'État partie comme condition pour exercer son activité sur ce territoire, tant que les autorités de régulation financière de l'État partie ont, à des fins de régulation et de surveillance, un accès immédiat, direct, complet et permanent aux informations traitées ou stockées sur les installations informatiques de services financiers que le fournisseur de services financiers couvert utilise ou implante en dehors du territoire de l'État partie. [46]

3.2.4. IDENTITÉ NUMÉRIQUE

L'identification numérique est non seulement étroitement liée à la question des données à caractère personnel, mais elle peut également avoir un impact majeur sur la distribution. Garantir l'accès de tous à l'identification est l'une des cibles des objectifs de développement durable (ODD), l'objectif 16.9, qui consiste à « fournir une identité légale à tous, y compris l'acte de naissance » d'ici à 2030. En outre, l'identification a permis l'accès aux opportunités financières et économiques, à la protection sociale, aux soins de santé, à l'éducation, etc. (World Bank, 2023). Les systèmes d'identification numérique peuvent soutenir le système d'identification sur papier, actuellement à la traîne. Cela est d'autant plus important dans le contexte de l'Afrique subsaharienne, qui compte près de 500 millions de personnes, soit près de la moitié de la population mondiale non enregistrée (World Bank, 2023).

La mise en place d'un système d'identification numérique est une tâche difficile, car elle nécessite de s'attaquer à la fois aux risques liés à la protection de la vie privée, à l'inclusivité et à la durabilité du système d'identification traditionnel (World Bank, 2023), ainsi qu'au risque de cybersécurité d'un système numérique (Kanwar, Reddy, Kedia, & Manish, 2022). Par conséquent, les particularités de la conception et de l'exploitation du système devront relever du gouvernement (d'où le droit de réglementer dans le contexte des accords régionaux). Toutefois, pour que les avantages du système d'identification numérique soient largement répandus, il convient de mettre l'accent sur la reconnaissance mutuelle des identités numériques, qui peut favoriser l'intégration et la coopération économiques régionales. Ceci est d'autant plus crucial pour réaliser les objectifs de la Communauté économique africaine assortis des libertés de circulation des personnes, des biens, des services et des capitaux.[47] Le Cadre d'interopérabilité de l'UA sur l'identification numérique et le Cadre stratégique en matière des données de l'UA reconnaissent et visent à atteindre un niveau élevé d'interopérabilité et de cohérence des systèmes d'identification numérique et de données à travers le continent.

45 Paragraphe 10, section B.2.3, projet de texte de négociation pour les Négociations de l'OMC sur le commerce électronique.
46 Paragraphe 10, section B.2.3, projet de texte de négociation pour les Négociations de l'OMC sur le commerce électronique.
47 Article 4.2.1, *Traité d'Abuja*.

Bien que plusieurs pays africains aient introduit des systèmes d'identification numérique, des systèmes d'identification numérique généralisés et interopérables restent un défi social et économique majeur sur le continent. Pour favoriser la reconnaissance mutuelle, le Cadre d'interopérabilité de l'identification numérique sera essentiel pour faciliter la création d'ensembles de données susceptibles de soutenir le développement de services publics et privés en Afrique.

Les considérations ci-dessus se reflètent dans les règles existantes concernant les identités numériques dans les cadres des ACR. Les dispositions relatives à l'identification numérique soulignent généralement le droit des États parties à réglementer la mise en œuvre nationale de systèmes d'identification numérique, tout en promouvant des mécanismes de soutien à l'interopérabilité et à la reconnaissance mutuelle entre les Parties. Les options ci-dessous sont donc prévues pour les dispositions relatives à l'identification numérique du protocole de la ZLECA sur le commerce numérique.

(I) ASPIRATION À PROMOUVOIR L'INTEROPÉRABILITÉ DES SYSTÈMES D'IDENTIFICATION NUMÉRIQUE

Reconnaissant que la coopération des États parties en matière d'identités numériques, individuelles ou d'entreprise, renforcera la connectivité régionale et mondiale, et reconnaissant que chaque État partie peut avoir des mises en œuvre et des approches juridiques différentes en matière d'identités numériques, chaque État partie s'efforce de promouvoir l'interopérabilité entre leurs systèmes respectifs d'identification numérique. [48]

(II) MESURES VISANT À PROMOUVOIR L'INTEROPÉRABILITÉ POUR L'IDENTIFICATION NUMÉRIQUE

Les États parties s'efforcent de faciliter les initiatives visant à promouvoir cette compatibilité et cette interopérabilité [entre les systèmes d'identification numérique], qui peuvent inclure :

a. l'établissement ou le maintien de cadres appropriés pour favoriser l'interopérabilité technique ou les normes communes entre la mise en œuvre des identités numériques par chaque État partie ;
b. la protection comparable des identités numériques offerte par les cadres juridiques respectifs de chaque État partie, ou la reconnaissance de leurs effets juridiques et réglementaires, qu'ils soient accordés de manière autonome ou d'un commun accord ;
c. l'établissement ou le maintien de cadres continentaux et internationaux plus larges [sur les systèmes d'identification numérique] ;
d. l'identification et la mise en œuvre des cas d'utilisation pour la reconnaissance mutuelle des identités numériques et
e. l'échange de connaissances et de l'expertise sur les meilleures pratiques relatives aux politiques et réglementations en matière d'identification numérique, à la mise en œuvre technique et aux normes de sécurité, ainsi qu'à la promotion de l'utilisation des identités numériques. [49]

48 Sur la base de l'article 7.1 de l'APEN ; article 8.61-S (1), le DEA entre le Royaume-Uni et Singapour.
49 Sur la base de l'article 7.1 de l'APEN ; article 8.61-S (2), le DEA entre le Royaume-Uni et Singapour.

(III) DÉLIMITER LES OBJECTIFS DE POLITIQUE PUBLIQUE

Il est entendu que rien dans le présent Article n'empêche un État partie d'adopter ou de maintenir des mesures incompatibles avec [*des mesures favorisant l'interopérabilité entre les systèmes d'identification numérique*] pour atteindre un objectif légitime de politique publique.[50]

3.2.5. DONNÉES PUBLIQUES OUVERTES

Les mégadonnées et les données ouvertes constituent les deux évolutions majeures qui façonnent la trajectoire de l'économie fondée sur les données. Les mégadonnées sont surtout utiles, et offrent la plus grande valeur économique et sociale, lorsqu'elles se présentent également sous forme de Données ouvertes (Gurin, 2014). Les données publiques ouvertes, qu'il s'agisse de mégadonnées ou non, peuvent contribuer à bâtir une société transparente, à renforcer la confiance et à permettre une utilisation plus intelligente des données en autorisant les individus, les organisations et même les gouvernements eux-mêmes à innover et à collaborer selon de nouvelles méthodes (World Bank, 2019; HM Government, 2013). Par exemple, les données publiques peuvent être utilisées dans le développement d'applications visant à améliorer l'accès et l'utilisation de services locaux tels que les transports publics (Gurin, 2014). McKinsey (2013) estime que les données ouvertes peuvent aider à libérer jusqu'à 5 000 milliards de dollars de valeur économique par an dans sept secteurs (éducation, transports, produits de consommation, électricité, pétrole et gaz, soins de santé et crédit à la consommation).

Le Cadre stratégique en matière des données de l'UA encourage la mise en place d'initiatives de données publiques ouvertes par les agences gouvernementales à l'appui de la création de systèmes de données nationaux intégrés et interopérables. Le Cadre stratégique en matière des données de l'UA souligne que « les normes de données ouvertes devraient être une priorité pour la création et la gestion des données publiques. La création de données selon ces normes n'exclut pas la superposition de mécanismes de contrôle ou de limitation d'accès dans des catégories de données définies à des fins justifiées ». En fait, plusieurs innovations réussies basées sur des données ouvertes ont été réalisées en Afrique en vue d'améliorer les performances dans les domaines de la production agricole, du social et de la gouvernance, ainsi que de l'accès aux médicaments.

Les données ouvertes entraîneraient des changements substantiels dans les aspects juridiques, sociaux et techniques (tels que des changements de mentalité ou des changements en termes d'approche de la gouvernance et du cadre juridique) (Open Data Handbook, 2023). De plus, il ne faut pas s'attendre à ce que la pratique des données ouvertes s'enracine automatiquement dans l'ensemble des institutions gouvernementales. Il est probable qu'il y ait une résistance au changement, et dans ce cas, il serait utile d'élaborer une campagne d'information et de sensibilisation aux données ouvertes pour tous les acteurs institutionnels (Schalkwyk, Willmers, & Schonwetter, 2015).

En conséquence, au niveau bilatéral, la plupart des dispositions relatives aux données publiques ouvertes figurant dans les ACR existants sont peu contraignantes. Elles représentent déjà une étape « réellement innovante et très pertinente » dans le domaine des régimes nationaux de gouvernance des données (Burri, 2021). Habituellement, les dispositions relatives aux

50 Basé sur l'article 7.2 de l'APEN.

données publiques ouvertes prévoient la reconnaissance des avantages conférés par l'accès du public aux données publiques et par leur utilisation, les critères possibles pour que les données publiques ouvertes soutiennent l'accès et l'utilisation, l'encouragement de la coopération bilatérale/régionale, ainsi que des domaines de coopération. Parmi ceux-ci, les critères pour les données publiques ouvertes peuvent soutenir la création de systèmes de données nationaux intégrés et interopérables visant à favoriser une économie des données solide, comme prévu dans le Cadre stratégique en matière des données de l'UA. Sur la base de l'examen des pratiques actuelles, quelques options sont proposées ci-après pour ces types de dispositions relatives aux données publiques ouvertes du Protocole de la ZLECAf sur le commerce numérique.

(I) ENCOURAGER L'ACCÈS DU PUBLIC AUX DONNÉES PUBLIQUES ET À LEUR UTILISATION

Les États parties reconnaissent que le fait de faciliter l'accès du public aux données publiques et leur utilisation favorise le développement économique et social, la compétitivité et l'innovation.[51] À cette fin, les États parties [*sont encouragés à / doivent s'efforcer d' / doivent*] étendre la couverture de ces données, notamment par l'implication et la consultation des parties prenantes intéressées.[52]

(II) CRITÈRES POUR LES DONNÉES PUBLIQUES OUVERTES

Dans la mesure où un État Partie décide de rendre les données publiques disponibles numériquement pour un accès et une utilisation publics, un État Partie [*doit s'efforcer de / doit*], dans la mesure du possible, s'assurer que ces données :

a. sont mises à disposition dans un format lisible par machine et ouvert ;

b. peuvent faire l'objet de recherches, être récupérées, utilisées, réutilisées et redistribuées ;

c. sont mises à jour, le cas échéant, en temps opportun ;

d. sont accompagnées de métadonnées qui sont, dans la mesure du possible, basées sur des formats couramment utilisés qui permettent à l'utilisateur de comprendre et d'utiliser les données ;

e. sont mises à disposition dans un format spatialisé avec des interfaces de programmation d'application (« API ») fiables, faciles à utiliser et accessibles gratuitement ;

f. sont généralement disponibles gratuitement ou à un coût raisonnable pour l'utilisateur ;

g. peuvent être utilisées à des fins commerciales et non commerciales, y compris dans le processus de production d'un nouveau produit ou service.[53]

51 Basé sur l'article 19.18.1 de l'ACEUM ; l'article 9.5.1 de l'APEN ; et l'article 8.61-H (1) de l'Accord sur l'économie numérique conclu entre le Royaume-Uni et Singapour (le DEA R.-U.-Singapour).

52 Paragraphe 2, Section B.4.1, Projet de texte de négociation pour les Négociations de l'OMC sur le commerce électronique.

53 Consolidé à partir de plusieurs textes de l'article 8.61-H (2) du DEA R.-U.-Singapour ; des paragraphes 3 et 4 de la section B.4.1 du projet de texte de négociation pour les Négociations de l'OMC sur le commerce électronique.

(III) ENCOURAGER LA COOPÉRATION AFIN DE FACILITER L'UTILISATION DES DONNÉES PUBLIQUES

Les États parties [*doivent s'efforcer de / doivent*] coopérer sur les questions qui facilitent et étendent l'accès du public aux données publiques et leur utilisation, y compris l'échange d'informations et d'expériences sur les pratiques et les politiques, en vue d'encourager le développement du commerce électronique et de créer des opportunités commerciales, notamment pour les petites et moyennes entreprises.[54]

(IV) DOMAINES DE COOPÉRATION

La coopération au titre du présent Article peut inclure des activités telles que les suivantes :

a. identifier conjointement les secteurs dans lesquels des ensembles de données ouvertes, notamment ceux qui ont une valeur mondiale, peuvent être utilisés afin de faciliter les transferts de technologie, la formation de talents et l'innovation, entre autres ;

b. encourager le développement de nouveaux produits et services basés sur des ensembles de données ouvertes ; et

c. favoriser l'utilisation et le développement des modèles de licences de données ouvertes sous la forme de licences publiques standardisées disponibles en ligne qui permettront aux données ouvertes d'être accessibles gratuitement, utilisées, modifiées et partagées par quiconque à toutes fins autorisées par les lois et réglementions respectives des États parties, et qui s'appuient sur des formats de données ouvertes.[55]

3.2.6. INNOVATION FONDÉE SUR LES DONNÉES

Les progrès technologiques intégrés dans la société moderne ont donné lieu à des ensembles de données plus nombreux et de meilleure qualité à utiliser et à analyser et qui, à leur tour, soutiennent l'amélioration de la prise de décision dans les secteurs public et privé. En outre, les données peuvent également être utilisées afin de soutenir d'autres innovations, telles que l'apprentissage automatique, l'automatisation et l'intelligence artificielle (IA) (Borne, 2021). Outre les opportunités offertes par l'application de l'IA à des données à grande échelle, les impacts socio-économiques qui en découlent suscitent des préoccupations croissantes. Ces préoccupations vont des pertes d'emplois possibles, de l'expansion du monopole avec un accès exclusif à la technologie, des impacts sur les droits humains fondamentaux et sur la stabilité politique, aux préoccupations éthiques liées aux erreurs d'algorithme et aux préjugés (Mittelstadt, 2021; Bossmann, 2016; Smart Africa Alliance, 2021; Adams, 2022).[56] Probablement en raison de ces préoccupations, ainsi que du fait que les pays se trouvent à différents stades de développement de l'innovation fondée sur les données, les dispositions relatives à l'innovation fondée sur les données dans les cadres régionaux et bilatéraux existants sont principalement conçues en termes d'« obligation de moyens » et de coopération, sans être juridiquement contraignantes (comme évoqué ci-dessous). En Afrique, le cadre stratégique en matière des données de l'UA souligne également l'importance de la nécessité d'une

54 Basé sur l'article 8.61-H (3) du DEA R.-U.-Singapour ; l'article 9.5.3 de l'APEN ; l'article 19.18.3 de l'ACEUM ; le paragraphe 5 de la section B.4.1 du projet de texte de négociation pour les Négociations de l'OMC sur le commerce électronique.

55 Article 9.5 de l'APEN.

56 Ce sujet sort du cadre du présent guide et ne sera pas exploré ici, car il a été traité dans d'autres initiatives panafricaines telles que la stratégie continentale de l'Union africaine sur l'intelligence artificielle (UA-IA) pour l'Afrique, qui est en cours de développement (AUDA-NEPAD, 2023), ou le Schéma directeur sur l'intelligence artificielle pour l'Afrique, développé conjointement par l'Alliance Smart Africa et le gouvernement sud-africain (Smart Africa Alliance, 2021).

réglementation économique afin de remédier à la répartition inégale des opportunités liées à la création de valeur et à l'innovation dans le domaine des données (African Union, 2022).

Alors que le secteur privé, étant le secteur le plus agile et le plus actif, devrait être le moteur d'une grande partie des progrès à venir, les gouvernements ont aussi un rôle important à jouer pour soutenir l'innovation fondée sur les données pour la croissance économique et l'amélioration de la qualité de vie. Les gouvernements ont, notamment, un rôle important à jouer dans la collecte et la diffusion des données, dans la création des cadres juridiques appropriés afin de favoriser le partage des données, et dans la sensibilisation du public à l'importance du partage des données (Castro & Korte, 2013). Le Cadre stratégique en matière des données de l'UA recommande la création d'un « Forum annuel d'innovation des données pour l'Afrique qui servira de plateforme pour des discussions multipartites, facilitera les échanges entre les Pays et sensibilisera les décideurs politiques sur le potentiel des données comme moteur de l'économie numérique actuelle. » Cela nécessite des actions de coopération entre toutes les parties prenantes, tant les gouvernements que les entreprises, afin de faire avancer l'économie d'innovation fondée sur les données.

La même notion est prise en compte dans la structure des dispositions des ACR relatives à l'innovation fondée sur les données. En règle générale, les dispositions relatives à l'innovation fondée sur les données reconnaissent le rôle des données et de l'innovation fondée sur les données dans l'économie et appellent à des activités de coopération afin de soutenir l'innovation fondée sur les données. Il convient de noter qu'à ce stade, comme dans d'autres domaines liés aux données, compte tenu des différentes approches en matière de gouvernance des données, les engagements en faveur de l'innovation des données sont principalement limités à une obligation de moyens. Sur la base de l'examen des pratiques actuelles, quelques options sont présentées ci-après pour les dispositions en matière d'innovation des données du Protocole de la ZLECAf sur le commerce numérique.

(I) RECONNAÎTRE LE RÔLE DES DONNÉES DANS L'ÉCONOMIE :

[Option 1] Les États parties reconnaissent que la numérisation et l'utilisation des données favorisent la croissance économique.[57]

[Option 2] Les États parties reconnaissent que la circulation transfrontalière des données et le partage des données favorisent l'innovation fondée sur les données.

(II) RECONNAÎTRE LA NÉCESSITÉ D'UN ENVIRONNEMENT ET DE MÉCANISMES PROPICES À L'INNOVATION DES DONNÉES

[Option 1] Pour soutenir le transfert transfrontalier d'informations par voie électronique et promouvoir l'innovation fondée sur les données, les États parties reconnaissent la nécessité de créer un environnement qui facilite, soutient et favorise l'expérimentation et l'innovation, notamment par l'utilisation de bacs à sable réglementaires, le cas échéant.[58]

[Option 2] Les États parties reconnaissent que l'innovation peut être améliorée dans le contexte de bacs à sable de données réglementaires où les données, y compris les informations personnelles, sont partagées entre les entreprises conformément aux lois et réglementations respectives des États parties.[59]

57 Article 8.61-I(1) du DEA R.-U.-Singapour.
58 Article 8.61-I (2) du DEA R.-U.-Singapour.
59 Based on Article 9.4.1, DEPA.

[Option 3] Les États parties reconnaissent que les mécanismes de partage de données, tels que les cadres de partage de données fiables et les accords de licence ouverts, facilitent le partage de données et encouragent leur utilisation dans l'environnement numérique afin de : a) promouvoir l'innovation et la créativité ; b) faciliter la diffusion de l'information, des connaissances, de la technologie, de la culture et des arts ; et c) favoriser la concurrence et les marchés ouverts et efficaces.[60]

(III) COLLABORATION SUR L'INNOVATION DES DONNÉES

Les États parties doivent s'efforcer de soutenir l'innovation des données par les actions suivantes :[61]

a. collaborer à des projets de partage de données, y compris des projets impliquant des chercheurs, des universitaires et l'industrie, en utilisant des bacs à sable réglementaires au besoin afin de démontrer les avantages liés aux transferts transfrontaliers d'informations par voie électronique ;[62]
b. coopérer à l'élaboration de politiques et de normes pour la mobilité des données, y compris en matière de portabilité des données des utilisateurs ; et
c. partager les approches politiques et les pratiques du secteur liées au partage de données, telles que les fiducies de données.[63]

3.2.7. INCLUSION NUMÉRIQUE

L'inclusion numérique est définie comme étant « un accès équitable, significatif et sûr à l'utilisation, à la direction et à la conception des technologies numériques, des services et des opportunités associées pour tous et partout » (United Nations, 2023). Il est sans doute approprié d'aborder l'inclusion numérique dans le contexte des questions liées aux données, car l'inclusion numérique se présente à la fois comme un défi et comme un résultat attendu de l'économie fondée sur les données. Les Nations unies mettent l'accent sur les facteurs d'accès, d'abordabilité et de participation lorsqu'il s'agit de contribuer à l'inclusion numérique (United Nations, 2023). Ces facteurs sont interdépendants, car l'accès et l'abordabilité fourniront aux individus les moyens de faire entendre leur voix et de participer.

Dans le contexte de l'Afrique, il est encore plus essentiel d'assurer l'inclusion numérique afin de garantir que le continent puisse tirer parti de l'économie fondée sur les données. L'IFC et Google estiment que l'économie liée à l'Internet en Afrique est susceptible d'atteindre 180 milliards de dollars américains d'ici 2025 et 712 milliards de dollars américains d'ici 2050 (Google & IFC, 2020). D'ailleurs, la Stratégie de transformation numérique pour l'Afrique (2020-2030) et le Cadre stratégique en matière des données de l'UA soulignent le fait que l'inclusion équitable est une condition importante pour l'économie des données. Cependant, afin de réaliser ce potentiel, le continent doit surmonter plusieurs défis liés aux infrastructures, aux ressources humaines et au cadre réglementaire.

60 Basé sur l'article 9.4.2 de l'APEN.
61 Article 8.61-I (3) du DEA R.-U.-Singapour
62 Il existe une disposition similaire dans l'article 9.4.3 de l'APEN.
63 Une fiducie de données peut être définie comme un mécanisme d'administration qui gère les données d'une personne en son nom. Cf. (Artyushina, 2021).

Les dispositions des ACR relatives à l'inclusion numérique visent à relever certains des défis liés à l'accès et à la participation à l'économie numérique et fondée sur les données grâce à une approche principalement coopérative. Cela inclut, entre autres, le partage des expériences et des meilleures pratiques, la suppression des obstacles à l'accès et le développement des compétences numériques. En outre, pour un meilleur suivi et un meilleur pilotage des politiques en faveur de l'inclusion numérique, le rôle de la collecte des données sous des formes désagrégées est également souligné en vue de fournir une base probante dans la formulation de politiques soutenant les inclusions numériques.

Sur la base de l'examen des pratiques actuelles, quelques options sont présentées ci-après pour les dispositions en matière d'innovation des données du Protocole de la ZLECAf sur le commerce numérique.

(I) RECONNAÎTRE L'IMPORTANCE DE L'INCLUSION NUMÉRIQUE

Les États parties reconnaissent l'importance de l'inclusion numérique afin de garantir que toutes les personnes et toutes les entreprises disposent de ce dont elles ont besoin pour participer à l'économie numérique, y contribuer et en bénéficier.[64]

Les États parties reconnaissent qu'il est important d'élargir et de faciliter les opportunités dans l'économie numérique en supprimant les obstacles à sa participation, et que cela peut nécessiter des approches sur mesure élaborées en consultation avec des personnes morales, des individus et d'autres groupes qui sont confrontés de manière disproportionnée à ces obstacles, et notamment les peuples autochtones, les femmes, les populations rurales et les groupes socio-économiques défavorisés.[65]

(II) DOMAINES DE COOPÉRATION POUR LE SOUTIEN À L'INCLUSION NUMÉRIQUE

À cette fin, les États parties coopèrent sur les questions relatives à l'inclusion numérique, y compris en ce qui concerne la participation des femmes, des populations rurales, des groupes socio-économiques défavorisés et des peuples autochtones à l'économie numérique. Cette coopération peut inclure les actions suivantes :

a. partager des expériences et de bonnes pratiques, y compris l'échange d'experts, en matière d'inclusion numérique ;

b. promouvoir une croissance économique inclusive et durable, afin de contribuer à garantir que les avantages de l'économie numérique soient plus largement partagés ;

c. identifier et éliminer les obstacles à l'accès aux opportunités de l'économie numérique ;

d. élaborer des programmes visant à promouvoir la participation de tous les groupes à l'économie numérique ;

e. améliorer les compétences numériques et l'accès aux outils commerciaux en ligne ;

f. promouvoir la protection du travail pour les travailleurs qui participent au commerce numérique ou qui le soutiennent ;

64 Basé sur l'article 11.1.1 de l'APEN.
65 Consolidé sur la base de l'article 11.1.2 de l'APEN et de l'article 8.61-P (1) du DEA R.-U.-Singapour.

g. partager les méthodes et procédures de collecte de données désagrégées, d'utilisation des indicateurs et d'analyse des statistiques liées à la participation à l'économie numérique ;

h. partager les meilleures pratiques, collaborer à des initiatives de renforcement des capacités, participer activement aux instances internationales et promouvoir la participation et la contribution des pays à l'élaboration mondiale de règles sur le commerce numérique ; et

i. d'autres domaines d'action convenus conjointement par les États parties.[66]

(III) MÉCANISME DE COOPÉRATION

Les activités de coopération relatives à l'inclusion numérique peuvent être menées par le biais d'une coordination, le cas échéant, des agences respectives des États parties, de leurs entreprises et syndicats, de la société civile, des institutions universitaires et des organisations non gouvernementales de ces derniers, entre autres. [67]

3.2.8. COOPÉRATION

Bien que les actions de coopération aient été couvertes par certaines des dispositions ci-dessus, il est possible d'avoir une disposition distincte qui recoupe tous les domaines soutenant les objectifs plus vastes de développement du commerce numérique, y compris les questions relatives aux données. Comme indiqué, la gouvernance des données reste un domaine politique sensible, notamment en ce qui concerne les données à caractère personnel, et nécessite, donc, une approche prudente permettant de concilier les avantages des différentes parties prenantes. En outre, la sécurité des données et le renforcement de la confiance constituent des éléments importants lorsqu'il s'agit de persuader les entreprises et les particuliers de participer à l'économie numérique. Alors que les solutions technologiques apportent la réponse à la sécurité des données, le renforcement de la confiance nécessite une approche progressive basée sur la coopération et la sensibilisation.

Les dispositions relatives à la coopération sont généralement énoncées sous la forme d'engagements d'« *obligation de moyens* » dans tous les ACR, comme l'indique l'utilisation de l'expression « *Les Parties doivent s'efforcer de [...].* » Cela indique le caractère peu contraignant de ce type de dispositions ainsi que la dépendance vis-à-vis des Parties pour ce qui est de mener à bien les activités prévues dans les dispositions. Les variables qui existent entre les différents ACR en ce qui concerne ce type de disposition ont trait aux domaines de coopération identifiés dans l'accord et au mécanisme de coopération. Vous trouverez ci-dessous la consolidation des domaines de coopération telle qu'énoncée dans l'accord commercial le plus complet avec un chapitre / des dispositions sur le commerce numérique à examiner dans le cadre du Protocole de la ZLECAf sur le commerce numérique. Les États parties peuvent ensuite ajouter ou supprimer des domaines qu'ils jugent adaptés à leurs aspirations.

(I) DOMAINES DE COOPÉRATION

Les États parties doivent s'efforcer :

a. d'échanger des informations et de partager des expériences sur les réglementations, les politiques, l'application et la conformité relatives à la protection des informations personnelles en vue de renforcer les mécanismes internationaux existants de coopération dans la mise en vigueur des lois sur la protection de la vie privée ;

66 Sur la base de l'article 11.1.3 de l'APEN et de l'article 8.61-P (2) et (4) du DEA R.-U.-Singapour.
67 Sur la base de l'article 11.1.4 de l'APEN et de l'article 8.61-P (3) du DEA R.-U.-Singapour.

b. de coopérer et de maintenir un dialogue sur la promotion et le développement de mécanismes qui favorisent l'interopérabilité continentale des régimes de protection de la vie privée ;

c. de promouvoir, par le biais d'initiatives internationales de coopération transfrontalière, le développement de mécanismes visant à aider les utilisateurs à déposer des plaintes transfrontalières concernant la protection des informations personnelles.[68]

d. d'identifier conjointement les secteurs dans lesquels les ensembles de données ouvertes, en particulier ceux qui ont une valeur mondiale, peuvent être utilisés afin de faciliter les transferts de technologie, la formation de talents et l'innovation, entre autres ;

e. d'encourager le développement de nouveaux produits et services basés sur des ensembles de données ouvertes ; et

f. de favoriser l'utilisation et de développer des modèles de licences de données ouvertes sous la forme de licences publiques standardisées disponibles en ligne, qui permettront aux données ouvertes d'être accessibles gratuitement, utilisées, modifiées et partagées par quiconque à toutes fins autorisées par les lois et réglementations respectives des États parties, et qui s'appuient sur des formats de données ouvertes.[69]

(II) MÉCANISME DE COOPÉRATION

Les États parties doivent [*envisager de créer / créer] un [forum / groupe de travail technique / sous-comité au sein du comité du commerce numérique / autres choix de mécanisme de coopération*] afin de traiter l'une des questions énumérées ci-dessus ou toute autre question relative au fonctionnement du présent Chapitre.[70]

3.2.9. EXCEPTIONS GÉNÉRALES

Outre la création d'un environnement propice à l'innovation et à la technologie numérique, les autres tâches essentielles des gouvernements concernent la promotion et la protection de la santé publique, la sécurité des utilisateurs, la moralité publique, l'ordre public, la sécurité nationale, etc. Afin de protéger et de promouvoir ces valeurs et ces intérêts d'ordre sociétal, les gouvernements conservent généralement le pouvoir d'adopter des lois ou de prendre d'autres mesures incompatibles avec les engagements susmentionnés. Celles-ci sont souvent prévues dans la clause des « Exceptions générales » des accords commerciaux, clause qui s'applique à l'ensemble de l'accord ou à un chapitre spécifique.

[Option 1] Incorporation de l'exception générale du GATT et du GATS : Aux fins du présent Accord, l'article XX du GATT de 1994 et sa note interprétative, et l'article XIV de l'Accord général sur le commerce des services figurant à l'annexe 1B de l'Accord sur l'OMC entrent en vigueur dans la mesure où ils sont applicables. À cette fin, les dispositions ci-dessus sont incorporées et font partie intégrante du présent Accord, mutatis mutandis. Les États parties conviennent en outre que, compte tenu des défis posés par le caractère mondial de l'Internet, le présent Accord n'empêche pas les Membres d'adopter ou de maintenir des mesures aux fins de garantir la cybersécurité, de sauvegarder la souveraineté du cyberespace, de protéger les droits et intérêts légitimes de leurs citoyens, personnes morales et autres organisations et d'atteindre d'autres objectifs légitimes de politique publique, à condition que ces mesures ne

68 Basé (en partie) sur l'article 19.14 de l'ACEUM
69 Basé sur l'article 9.5.4 de l'APEN..
70 Basé sur l'article 19.14 de l'ACEUM.

soient pas appliquées d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable ou une restriction déguisée au commerce, et ne soient pas plus que nécessaires pour atteindre les objectifs.[71]

[Option 2] Spécifier les exceptions : Sous réserve que ces mesures ne soient pas appliquées d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable entre des pays où des conditions similaires existent, ou une restriction déguisée au commerce et au transfert transfrontalier d'informations par voie électronique, rien dans le présent Accord n'est interprété comme empêchant l'adoption ou l'application par tout État partie de mesures : a) nécessaires afin de protéger la moralité publique ou de maintenir l'ordre public ; b) nécessaire afin d'assurer l'imposition ou la perception équitable ou efficace d'impôts directs sur le commerce par des moyens électroniques ; c) nécessaires afin de garantir le respect des lois ou réglementations qui ne sont pas incompatibles avec les dispositions du présent Accord, y compris celles qui sont relatives à : i) la prévention des pratiques trompeuses et frauduleuses ; ii) la protection de la vie privée des personnes en relation avec le traitement et la diffusion des données à caractère personnel et la protection de la confidentialité des documents et comptes individuels ; et iii) la sécurité.[72]

3.2.10. PRÉVENTION ET RÈGLEMENT DES DIFFÉRENDS

Les États parties peuvent décider d'appliquer ou non un mécanisme de règlement des différends (MRD) aux dispositions relatives aux données, et à l'ensemble du Protocole sur le commerce numérique. L'applicabilité des dispositions relatives aux données variera en fonction de la manière dont les dispositions relatives aux données sont structurées en combinaison avec l'applicabilité du MRD. Figure 9 ci-dessous illustre les différents niveaux d'applicabilité des dispositions de l'ACR par ordre croissant. Par exemple, une disposition contenant des aspirations (à savoir : Les États parties « devront », « doivent s'employer à », « doivent s'efforcer de », etc.) sera moins contraignante pour les États parties qu'une disposition dont le libellé est imprégné d'un plus fort engagement (à savoir : Les États parties « doivent », « doivent s'engager à », « ne doivent pas manquer de », etc.). Une disposition soumise au MRD est plus facilement exécutoire qu'une disposition qui n'est pas [soumise au MRD]. Cela nécessite de lire les dispositions dans leur contexte et en relation avec d'autres dispositions/chapitres de l'accord.

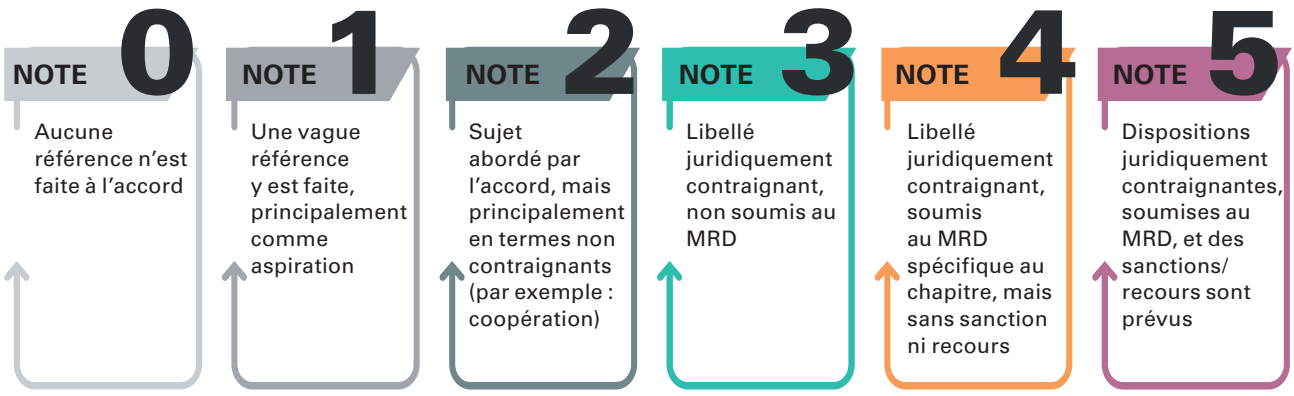
Les ACR actuels présentent différentes approches du MRD conformément aux dispositions relatives aux données. Le RCEP, par exemple, exclut actuellement du règlement des différends toutes les questions relevant de son Chapitre sur le commerce électronique. Le CPTPP, en revanche, prévoit une période de transition pour des membres spécifiques afin de leur donner le temps de nécessaire pour ajuster les réglementations nationales. L'APEN fournit un cadre complet pour la prévention et le règlement des différends en vertu du chapitre sur le commerce numérique, y compris toutes les étapes procédurales pour la réalisation d'une médiation et d'un arbitrage. Ce MRD exclut cependant explicitement son application à certaines des dispositions « sensibles », notamment le transfert transfrontalier d'informations par voie électronique et l'implantation des installations informatiques.

71 Sur la base de l'article 6 de l'annexe 1 : Champ d'application et dispositions générales, Projet de texte de négociation pour les Négociations de l'OMC sur le commerce électronique.

72 Sur la base de l'article 6 de l'annexe 1 : Champ d'application et dispositions générales, Projet de texte de négociation pour les Négociations de l'OMC sur le commerce électronique.

Lorsque le MRD est appliqué, ses dispositions permettent souvent la mise en œuvre d'un mécanisme de règlement des différends à plusieurs niveaux, dans lequel les Parties procèdent étape par étape en suivant un processus de règlement des différends à plusieurs niveaux. Le processus commence généralement par des consultations bilatérales, suivies d'autres modes alternatifs de règlement des différends (ADR) et se termine par un arbitrage / comité d'arbitrage avec une décision contraignante ou un rapport non contraignant sur les conclusions rendues. Vous trouverez ci-dessous les différentes options d'application du MRD aux dispositions relatives aux données, ainsi qu'au Protocole sur le commerce numérique. Lorsque le MRD est sélectionné comme méthode applicable [option 3 du type de disposition i)], d'autres types de dispositions (à partir de la disposition ii)] peuvent être prises en considération. Une disposition sur l'objectif du MRD est également prévue afin de souligner que les solutions mutuellement convenues constituent le meilleur résultat possible qui devra guider l'action de tous les États parties en cas de désaccord surgissant au cours de la mise en œuvre de l'Accord.

Illustration 9. Exemple de niveaux d'applicabilité des dispositions



Source : Basé sur (Baker, 2022 ; Baker, 2021)

(I) APPLICABILITÉ DU MÉCANISME DE RÈGLEMENT DES DIFFÉRENDS :

[Option 1] Exclus du MRD : Aucun État partie n'aura recours au règlement des différends en vertu du Chapitre [indiquer le numéro de chapitre] (Règlement des différends) pour toute question découlant du présent Chapitre.[73]

[Option 2] Mécanisme d'examen intégré pour l'inclusion des dispositions relatives aux données dans le MRD : Dans le cadre de tout examen général du présent Accord, les États parties doivent examiner l'application du Chapitre sur le Règlement des différends au présent Chapitre <identifier le numéro du chapitre> [*Commerce numérique, y compris la fourniture de données*]. À l'issue de l'examen, le chapitre sur le Règlement des différends s'applique au présent Chapitre entre les Parties qui ont convenu de son application. [74]

[Option 3] Application du MRD spécifique au Chapitre sur le Commerce numérique (y compris pour les dispositions relatives aux données) / MRD général : À l'exception de <*indiquer les dispositions à exclure du règlement des différends, le cas échéant*>, le mécanisme de règlement des différends prévu dans <*indiquer l'annexe ou le chapitre sur le règlement des différends*> s'applique :

73 Basé (en partie) sur l'article 12.17.3 du RCEP.
74 Basé (en partie) sur l'article 12.17.3 du RCEP.

a. à la prévention ou au règlement des différends entre les États parties en ce qui a trait à l'interprétation ou à l'application du présent Accord ; ou

b. lorsqu'un État partie considère qu'une mesure effective ou proposée d'un autre État partie est ou serait incompatible avec une obligation du présent Accord, ou qu'un autre État partie n'a pas respecté une obligation en vertu du présent Accord.[75]

(II) OBJECTIFS

Les États parties s'efforcent à tout moment de s'entendre sur l'interprétation et l'application du présent Accord et font tout ce qui est en leur pouvoir, par la coopération et par le biais de consultations, afin de parvenir à une résolution mutuellement satisfaisante de toute question susceptible d'affecter son fonctionnement.

L'objectif de ce [chapitre ou cette disposition sur la prévention et le règlement des différends] est de fournir un processus efficace, efficient et transparent pour les consultations et le règlement des différends entre les États parties concernant leurs droits et obligations en vertu du présent Accord.

(III) PÉRIODE TRANSITOIRE POUR CERTAINS ÉTATS PARTIES

<*Préciser l'État partie ou les États parties*> n'est ou ne sont pas soumis au règlement des différends en vertu du chapitre <*préciser le numéro du chapitre*> (Règlement des différends) en ce qui concerne ses/leurs obligations en vertu de l'article <*préciser le numéro de l'article*> pendant une période de <*préciser le nombre d'années de transition*> ans après la date d'entrée en vigueur du présent Accord pour <*préciser l'État partie ou les États parties*>.[76]

(IV) CONSULTATION

En cas de différend entre les États parties concernant l'interprétation et l'application du présent Chapitre, les États parties concernés doivent mener d'abord des consultations en toute bonne foi et s'efforcer de tout mettre en œuvre afin de parvenir à une solution mutuellement satisfaisante. Un État partie (État partie requérant) peut, à tout moment, demander des consultations avec un autre État partie (État partie répondant) concernant toute question soulevée dans le cadre du présent Chapitre en adressant une demande écrite à l'interlocuteur de l'État partie répondant. Si ces consultations ne parviennent pas à résoudre les différends, tout État partie engagé dans lesdites consultations pourra saisir le [*cadre institutionnel de l'Accord*].[77]

(V) BONS OFFICES ET CONCILIATION

Les États parties peuvent à tout moment convenir d'adopter volontairement toute méthode alternative de règlement des différends, telle que les bons offices ou la conciliation. Les procédures de bons offices ou de conciliation sont confidentielles et ne portent pas atteinte aux droits des Parties dans toute autre procédure. Les États parties participant à une procédure en vertu du présent article [Bons offices et conciliation] peuvent suspendre ou mettre fin à cette

75 Adapté de l'article 14.3 de l'APEN.
76 Basé sur l'article 14.18 du CPTPP.
77 Basé (en partie) sur l'article 12.17.2 du RCEP.

procédure à tout moment. Si les États parties en litige en conviennent, les bons offices ou la conciliation peuvent se poursuivre pendant que le différend est en cours de résolution devant un tribunal arbitral établi en vertu de l'article <identifier le numéro de l'article> (Tribunaux arbitraux).[78]

(VI) ARBITRAGE / COMITÉ D'ARBITRAGE

Si les États parties qui ont pris part aux consultations n'ont pas réussi à résoudre la question au plus tard <*indiquer le nombre de jours*> jours après la date de réception d'une demande de consultation, l'État partie requérant peut demander la constitution d'un [*tribunal arbitral / comité d'arbitrage*] en vertu de l'article <*indiquer le numéro de l'article*> (Création [*d'un tribunal arbitral / d'un comité d'arbitrage*]) et comme prévu au Chapitre <indiquer le numéro du chapitre> (Règlement des différends).

(VII) ÉLECTION DE FOR

Si un différend concernant une question quelconque surgit dans le cadre du présent Accord et d'un autre accord commercial international auquel les États parties en litige ont pris part, y compris l'Accord sur l'OMC, l'État partie plaignant peut élire le for dans lequel le différend sera réglé. Une fois qu'un État partie plaignant aura demandé l'établissement d'un comité d'arbitrage ou de tout autre tribunal arbitral en vertu d'un accord [comme susmentionné], ou aura renvoyé une question à celui-ci, le for choisi est utilisé à l'exclusion de tout autre for.[79]

78 Basé sur l'article 14.4 de l'APEN.
79 Basé sur l'article 14.7 de l'APEN.

Lectures supplémentaires

- Projet de texte de négociation en lien avec les négociations sur le commerce électronique de l'OMC. INF/ECOM/62/Rev.2. 8 septembre 2021.
- Accord de partenariat sur l'économie numérique (APEN) entre la Nouvelle-Zélande, le Chili et Singapour.
- Accord sur l'économie numérique (DEA) entre le Royaume-Uni de Grande-Bretagne, l'Irlande du Nord et la République de Singapour.
- Chapitre 14 (Commerce électronique), Accord de partenariat transpacifique global et progressiste.
- Chapitre 19 (Commerce numérique), Accord Canada–États-Unis–Mexique (ACEUM).
- Titre III (Commerce numérique), Accord de commerce et de coopération (ACC) entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et l'Irlande du Nord, d'autre part.
- Section F (Commerce électronique), Chapitre 8 (Services, Établissement et Commerce électronique), Accord de libre-échange (ALE) entre l'Union européenne et Singapour.
- Chapitre 12 (Commerce électronique), Partenariat économique régional global.
- Burri, M. (Ed.). (2021). « Big Data and Global Trade Law ». Cambridge : Cambridge University Press. DOI : 10.1017/9781108919234.

3.3 LIGNES DIRECTRICES À L'INTENTION DES NÉGOCIATEURS POUR LA PRISE EN COMPTE DES DISPOSITIONS LIÉES AUX DONNÉES DES PROTOCOLES DE LA ZLECAF EN MATIÈRE DE COMMERCE NUMÉRIQUE

3.3.1. CADRE INSTITUTIONNEL GÉNÉRAL

ORIENTATION GÉNÉRALE

Les pays disposent de différents modèles de cadres institutionnels pour mandater la responsabilité du ministère-chef de file en charge de la négociation commerciale et d'autres ministères sectoriels. Par exemple, tandis que certains pays désignent le ministère des Affaires étrangères comme ministère-chef de file, exploitant son réseau mondial ainsi que ses qualités diplomatiques, d'autres désignent le ministère du Commerce afin de tirer profit de ses connaissances spécialisées en matière de commerce (Baker P. R., Le, Vanzetti, & Ngov, 2022). Spécifique aux dispositions relatives aux données (y compris la protection des données, la circulation des données, les données gouvernementales ouvertes, etc.), les ministères des technologies de l'information et de la communication (TIC) devront piloter les aspects techniques. Les agences pour la protection des données, le cas échéant, devront également être étroitement impliquées durant la procédure. En ce qui concerne les identités numériques,

l'autorité nationale compétente en matière d'identification devra également être impliquée. En matière de vérification du texte de loi, le ministère de la Justice ou le département des Affaires juridiques des ministères compétents impliqués devra lui aussi être consulté. Pour résumer, le cadre institutionnel d'une politique commerciale doit toujours être en adéquation avec le programme économique intérieur global et le représentant désigné du pays.

Dans n'importe quelle négociation commerciale, la coordination et la consultation en interne entre les agences gouvernementales concernées et le secteur privé sont déterminantes pour sa réussite. Des consultations devront être menées régulièrement. Elles ne devront pas être réalisées avant le démarrage de la négociation afin que suffisamment d'informations puissent être collectées, par exemple les bénéfices potentiels, les préoccupations des secteurs privés, les enjeux en matière de mise en œuvre, etc. On peut également les utiliser afin de décider si un accord spécifique mérite d'être poursuivi et de fixer des lignes rouges (qui favoriseront la formation de la zone d'accord possible (ZOPA) ainsi que la meilleure alternative à un accord négocié (BATNA) pour l'équipe de négociation). Une fois les négociations conclues, des consultations internes appropriées peuvent aider les parties à mettre efficacement ces politiques en application et à bénéficier pleinement du potentiel de ces avantages.

L'IMPORTANCE DE LA COORDINATION ET DES CONSULTATIONS AU NIVEAU INTERMINISTÉRIEL

L'objectif des consultations entre les agences gouvernementales est de s'assurer qu'elles soient bien coordonnées en vertu de leurs mandats respectifs et qu'elles restent au service de l'objectif de développement « plus large » du pays. Sans cette consultation interne appropriée, il est possible que les négociateurs ne disposent pas d'informations nécessaires suffisantes pour négocier avec leurs homologues étrangers et prennent le risque de perdre de vue l'intérêt principal du pays. En outre, il y a de fortes chances que cela compromette la capacité de soutien politique au niveau national (UNCTAD, 2018).

Une consultation doit être réalisée régulièrement avant le début des négociations en vue de rechercher les éléments importants qui affectent certains domaines de l'accord, pour s'assurer que les objectifs généraux de la négociation soient menés à bien. On peut également l'utiliser pour répondre à la proposition du partenaire de négociation et ajuster une position de négociation sans perdre la majorité des avantages.

L'IMPORTANCE DE LA CONSULTATION AVEC LE SECTEUR PRIVÉ

La société civile et les associations de protection des consommateurs doivent être impliquées dans l'élaboration de la position nationale, tandis que les exploitants du secteur privé, qui ont une meilleure connaissance du marché ainsi que de la technologie soutenant les marchés de données, doivent être consultés et impliqués dans ce processus, car ce seront finalement les exploitants et régulateurs qui constitueront les principaux « utilisateurs » des dispositions relatives aux données stipulées dans les accords commerciaux. Le secteur privé, y compris les consommateurs, est le bénéficiaire final des accords commerciaux, en particulier lorsqu'il s'agit de protection des données. Ainsi, il doit être impliqué autant que possible dès le lancement de toute négociation commerciale. Le secteur privé ainsi que les représentants des associations de consommateurs constituent les sources principales de renseignements sur le terrain. Ils peuvent notamment fournir aux négociateurs des informations liées aux avantages et enjeux de l'utilisation des accords commerciaux, entre autres. Une consultation régulière et opportune du secteur privé peut également leur donner le temps d'être à même et,

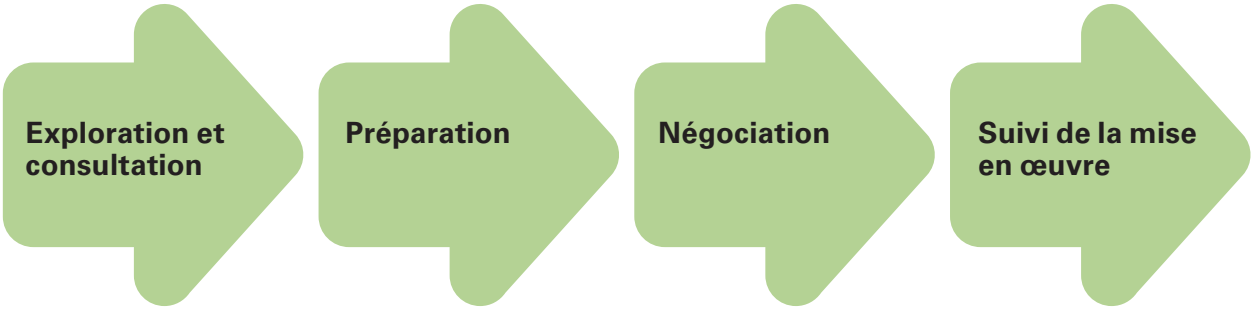
ainsi, d'être préparés à ce que le projet d'accord puisse être conclu par les pouvoirs publics. À l'inverse, cela ne servirait à rien qu'un accord conclu ne puisse pas être efficacement mis en œuvre par le secteur privé au niveau national.

3.3.2. CADRE ANALYTIQUE EN MATIÈRE DE NÉGOCIATION DES DISPOSITIONS RELATIVES AUX DONNÉES

Cette section propose une approche suggérée du cadre analytique en préparation de négociations commerciales, ainsi que des suggestions d'outils pouvant être utilisés à chaque étape du processus (Table 2). Cependant, il est important de noter que ceux-ci doivent être considérés comme des étapes d'analyse essentielles, mais qu'une analyse plus poussée (par exemple une évaluation à grande échelle de l'impact sur le développement durable et une consultation des parties prenantes au niveau national) doit être menée afin de garantir des observations plus holistiques des incidences éventuelles d'un accord négocié (Baker & Le, 2022) (European Commission, 2016). Les résultats provenant de ces outils doivent être lus et interprétés en combinaison avec les observations et l'expérience pratique, l'influence potentielle des forces politico-économiques et les visions pour le pays concernant le développement d'un partenariat stratégique avec les homologues considérés.

Comme souligné plus haut, différentes agences gouvernementales peuvent être impliquées dans ce processus. Il sera bénéfique que l'ensemble des agences s'accordent très tôt sur le mécanisme de communication et de coordination. Par exemple, le ministère du Commerce peut être chargé de la négociation de tout le chapitre dédié au commerce numérique, tandis que l'équipe technique sera composée de représentants du ministère des TIC et du DPA afin de garantir les données techniques.

Tableau 2. Cadre analytique en préparation de la négociation des dispositions relatives aux données



Étape	Travaux analytiques	Objectif	Outil analytique
Étape 1 : Exploration et consultation	Faire le bilan des cadres réglementaires existants en matière de données	• Faire le bilan des cadres réglementaires nationaux en matière de données et/ou du développement éventuel ou des modifications possibles dans le futur proche (sur le plan politique) • Identifier les priorités et les sujets de préoccupation des entreprises et individus au niveau national en matière de commerce/transfert transfrontalier des données • Profil réglementaire général des parties en matière de gouvernance des données pour savoir si des lois/réglementations existent en matière de gouvernance des données, orientation générale • Les engagements actuels proposés par d'autres parties concernant les domaines négociés dans les ACR existants (le cas échéant)	Outil Cyberlaw Tracker de la CNUCED Analyse du texte de loi Consultations
Étape 2 : Préparation	Propositions d'un texte de loi concernant les dispositions relatives aux données	Préparation des options de textes de loi concernant les dispositions relatives aux données en fonction de l'analyse menée au cours de l'étape d'exploration	Dossier sur la politique en matière de données Analyse du texte de loi
Étape 3 : Négociation	Révision des documents préparés à l'Étape 2	Révision en vue de refléter les modifications et nouvelles informations obtenues au cours des négociations.	Analyse du texte de loi
Étape 4 : Suivi de la mise en œuvre	Évaluation de la conformité et suivi	• Évaluation de la conformité des réglementations nationales vis-à-vis des dispositions négociées • Identification des éventuels domaines à modifier au sein des réglementations nationales • Mise en œuvre des modifications • Évaluation des enjeux de la mise en œuvre nécessitant d'être traités	Rapports des parties prenantes Consultations Cadre de suivi

4. CONCLUSIONS

Le développement au sein de l'économie mondiale est de plus en plus stimulé par les secteurs fondés sur les données de l'économie. Selon cette tendance, les données sont devenues un atout majeur qui a été standardisé et monétisé en vue de créer un nouveau flux de revenus pour les grandes entreprises (WEF, 2011; Sadowski, 2016). Les données sont désormais au cœur de nombreuses technologies de pointe qui propulsent l'économie numérique. Non seulement elles contribuent à la production de biens et services, mais elles possèdent également des caractéristiques uniques qui permettent aux entreprises de générer de nouveaux flux de revenus et de contribuer à leur compétitivité (Hagiu & Wright, 2020). Toutefois, il convient de souligner qu'il existe des inégalités en matière d'accès et de croissance des marchés de données, qui peuvent être résolues par des négociations commerciales et une gouvernance efficace des données (Union africaine, 2022).

La valeur des données est indiscutable, mais d'importantes divergences existent concernant les approches réglementaires. Les données devenant une contribution de plus en plus importante à l'offre de biens et services, l'utilisation d'analogies imparfaites de contributions historiques à la production pourrait apporter certaines suggestions sur la manière de les réguler. Cependant, même parmi les spécialistes, il existe de nombreux points de vue différents sur la manière de traiter des données : que cela relève du domaine professionnel, des fonds, des propriétés individuelles ou même du domaine infrastructurel (Aaronson, 2021). Ces différents points de vue, associés aux mesures d'incitation de type réglementaire, ont renforcé la divergence des approches en matière de gouvernance des données. Les trois plus importants marchés numériques (les États-Unis, l'Union européenne et la Chine) ont des approches différentes en matière de gouvernance des données. Les États-Unis se concentrent sur le contrôle des données par le secteur privé, la Chine met l'accent sur le contrôle des données par les pouvoirs publics, tandis que l'Union européenne favorise le contrôle des données par les individus sur la base des valeurs et droits fondamentaux (UNCTAD, 2021). Quel que soit le point de vue, le rôle joué par les pouvoirs publics est indéniable pour apporter un cadre réglementaire juste qui favorise une utilisation responsable, sécurisée et équitable des données. Ces considérations sont pertinentes en ce qui concerne l'Afrique, où les fragilités des cadres institutionnels, du développement humain et de la préparation au numérique empêchent les pays de tirer profit de l'énorme quantité de données générées par leurs institutions, leur secteur privé et leurs citoyens. La taille potentielle du marché et les avantages découlant des efforts d'harmonisation ont été reconnus dans le Cadre stratégique en matière des données de l'UA, où des interventions politiques clés visant à favoriser la circulation transfrontalière des données ont été identifiées et sont en cours de mise en œuvre.

De nouveaux modes d'utilisation des données nécessitent de nouvelles manières de penser les données. Les caractéristiques uniques des données indiquent qu'elles doivent être traitées différemment des biens et services conventionnels, notamment en ce qui concerne leurs transferts internationaux. Dans le nouveau contexte de l'économie numérique fondée sur les données, la CNUCED (2021) propose que les efforts politiques se concentrent sur le droit d'accès, le contrôle et l'utilisation des données plutôt que d'essayer de savoir qui « possède » les données. (UNCTAD, 2021). Outre les données utilisées dans le secteur privé, la création de valeur à partir des données publiques est également importante pour renforcer les intérêts publics en améliorant la fourniture de services sûrs et équitables.

Afin d'améliorer l'élaboration des réglementations qui régulent les données, les décideurs politiques devront reconnaître et s'accorder sur les caractéristiques singulières des données. À l'heure actuelle, il n'existe pas de définition officielle ni de taxonomie des données. En fonction de différents critères de sélection, des données peuvent être catégorisées comme données à caractère personnel ou non personnel, données sensibles ou non sensibles, données privées ou publiques, etc. (UNCTAD, 2021). Dans leur forme la plus pure, c.-à-d., de nombreux types de données possèdent les caractéristiques des biens publics (World Bank, 2021), ce qui nécessite en conséquence l'intervention des pouvoirs publics pour s'assurer de l'élimination efficace des externalités.

Parmi elles, les données à caractère personnel sont sans nul doute devenues une ressource importante qui nécessite une attention particulière (Ciuriak, 2018; WEF, 2011). L'utilisation des données à caractère personnel étant étroitement liée au respect de la vie privée et à la sécurité des individus, les citoyens doivent avoir la possibilité d'exprimer leur point de vue au cours du processus d'élaboration des règles afin de garantir la transparence, la participation et la responsabilisation des réglementations. Cela contribuera à l'élément « confiance » qui soutient la croissance de l'économie numérique et mettra d'abord l'accent sur la création d'un environnement réellement favorable, puis instaura la confiance en cette nouvelle économie en donnant aux individus du monde entier les moyens de contrôler leurs données.

Deux caractéristiques sont souhaitables en matière de réglementation de la gouvernance des données : permettre l'accès aux données et susciter la confiance. Un environnement favorable en matière d'utilisation et de circulation des données soutiendrait incontestablement l'innovation et créera davantage de valeur à la société que la somme de chaque point de données. Malgré tout, l'élément crucial de confiance serait altéré s'il n'y avait pas de mécanisme de détection et de prévention de l'usage impropre, de l'usurpation d'identité ou d'autres violations. Ainsi, il est important de garder à l'esprit que les données aident à stimuler l'innovation, mais que des limites doivent être posées afin de protéger la vie privée des citoyens ainsi que les intérêts financiers de l'État. Une approche équilibrée est fortement souhaitée, mais également difficile à atteindre. Cela nécessiterait de prendre en compte l'ensemble des conditions et intérêts de l'environnement national. Dans ce contexte, le Cadre stratégique en matière des données de l'UA souligne l'importance de créer des systèmes de données légitimes et fiables par la mise en œuvre d'un large éventail de mesures, comprenant non seulement la cybersécurité et la protection des données, mais aussi la promotion de la justice et de l'éthique en matière de données.

Bien qu'il soit difficile d'adopter un règlement unique pour tous, les États membres de l'UA devraient s'efforcer de parvenir à des normes et à des règles communes fondées sur les recommandations du Cadre stratégique en matière des données de l'UA et les dispositions de la Convention de Malabo en matière de protection des données à caractère personnel. Cela contribuera à la création d'un environnement numérique moins fragmenté, où « davantage d'individus auraient un meilleur accès à l'information, et où les individus pourraient créer et partager plus d'informations » (Aaronson, 2016). C'est là que les règles du commerce numérique, et plus particulièrement les dispositions relatives aux données, entrent en jeu. Comme abordé plus haut, tandis que les dispositions relatives aux données dans les ACR ne spécifient pas le niveau de détail fourni en matière de réglementations nationales applicables aux données, elles établissent les normes minimales tout en accordant aux États parties le pouvoir de déterminer la méthode appropriée de mise en œuvre des dispositions de l'accord dans leur propre système et pratique juridique. En outre, des considérations particulières telles qu'une période de transition et le développement des capacités doivent être présentées pour les États parties les moins avancés sur le plan numérique, afin de leur accorder un espace politique suffisant pour élaborer

la réglementation liée aux données conformément aux engagements tout en continuant de satisfaire leurs exigences nationales.

Les pays se trouvant à différentes étapes de l'élaboration des cadres de gouvernance des données, des actions collaboratives vont s'avérer nécessaires. Les pays en développement pourront bénéficier d'un engagement précoce dans les discussions régionales et plurilatérales en matière de circulation des données, afin de s'assurer que leurs voix sont entendues, et que leurs intérêts sont pris en considération. Cette participation anticipée et proactive des pays en développement leur donnera plus de poids dans le processus d'élaboration des règles, au lieu de la position classique en matière d'élaboration des règles. Cette approche pourra concilier les divergences en matière d'éthique d'utilisation des données, de désinformation et d'autres problématiques réglementaires afin de garantir que les données et que l'économie fondée sur les données soient atteintes au même titre qu'une croissance juste et équitable.

Ce guide de référence sur la façon de considérer et d'intégrer les dispositions relatives aux données dans la négociation des protocoles de commerce numérique au sein de la ZLECA a été préparé suivant ces caractéristiques de données, les bonnes pratiques tirées d'expériences mondiales ainsi que les principes de base précédemment mentionnés et conformes au cadre stratégique en matière des données de l'UA et à la stratégie de transformation numérique de l'Afrique. Les lignes directrices ont pour objectif d'aider les équipes de négociation à prendre en considération les dispositions liées aux données de base contenues dans les accords de libre-échange ainsi qu'à prendre en compte les implications économiques et sociétales plus larges de la prise d'engagements dans neuf domaines essentiels, afin de faire progresser le commerce numérique intra-africain ainsi que l'intégration régionale conformément aux objectifs de l'Agenda 2023 ainsi qu'à la langue faisant foi dans les dispositions en question. La nature de la gouvernance des données étant évolutive et dynamique, les informations contenues dans le guide de référence doivent être considérées en parallèle des nouvelles évolutions sur le marché des données et des réglementations en matière de données.

RÉFÉRENCES

Aaronson, S. A. (2016). *The Digital Trade Imbalance and Its Implications for Internet Governance.* The Digital Trade Imbalance and Its Implications for Internet Governance. Retrieved from *https://www.cigionline.org/publications/digital-trade-imbalance-and-its-implications-internet-governance/*

Aaronson, S. A. (2021). Data Is Different, So Policymakers Should Pay Close Attention to Its Governance. In M. Buri, *Big Data and Global Trade Law* (pp. 340-360). Cambridge University Press.

Adams, R. (2022, May 30). *AI in Africa: Key Concerns and Policy Considerations for the Future of the Continent*. Retrieved from Africa Policy Research Institute: *https://afripoli.org/ai-in-africa-key-concerns-and-policy-considerations-for-the-future-of-the-continent*

African Union. (2020). *The Digital Transformation Strategy for Africa (2020-2030).*

African Union. (2022). *AU Data Policy Framework.*

African Union. (2022). *Decision on the Reports of the Sub-Committees of the Permanent Representatives' Committee (PRC). 40th Ordinary Session of the Executive Council (02-03 February 2022).* Retrieved from *https://au.int/sites/default/files/decisions/41584-EX_CL_Dec_1143-1167_XL_E.pdf*

African Union. (2023). *List of Countries Which Have Signed, Ratified/Acceded To The African Union Convention On Cyber Security And Personal Data Protection.*

African Union Commission. (2018). *African Forum on Cybercrime: African Union Convention on Cybersecurity and Personal Data Protection.*

African Union. (forthcoming). *Draft Continental Harmonisation Strategy on Policy and Regulatory Environment for Africa's Digital Single Market.*

APEC. (2005). *APEC Privacy Framework*. APEC Secretariat. Retrieved from *https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf*

APEC. (2019). *What is the Cross-Border Privacy Rules System?* Asia-Pacific Economic Cooperation. Retrieved from *https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,2005%20and%20updated%20in%202015*

Arasasingham, A., & Goodman, M. P. (2023, April 13). Operationalizing Data Free Flow with Trust (DFFT). *CSIS*.

Artyushina, A. (2021, June 10). *The future of data trusts and the global race to dominate AI*. Retrieved from Bennett Institute for Public Policy of Cambridge: *https://www.bennettinstitute.cam.ac.uk/blog/data-trusts1/*

AUDA-NEPAD. (2023, March 29). *Artificial Intelligence is at the core of discussions in Rwanda as the AU High-Level Panel on Emerging Technologies convenes experts to draft the AU-AI Continental Strategy*. Retrieved from African Union Development Agency (AUDA-NEPAD): *https://www.nepad.org/news/artificial-intelligence-core-of-discussions-rwanda-au-high-level-panel-emerging*

Ayalew, Y. E. (2023, June 15). *The African Union's Malabo Convention on Cyber Security and Personal Data Protection entered into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?* Retrieved from European Journal of International Law Blog: *https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/*

Babalola, O. (2022). *Data Protection Legal Regime and Data Governance in Africa: An Overview.* AERC Africa.

Baker McKenzie. (2023, January 28). *Data Protection Day - Key developments and trends for 2023*. Retrieved from Lexology: *https://www.lexology.com/library/detail.aspx?g=e4ead5f0-ccd4-4762-8e06-7dd84c8341ff*

Baker, P. (2022). Trade and Sustainable Development in EU Economic Partnership Agreement. *Cross-Regional Exchange on Trade and Sustainable Development in EU Economic Partnership Agreement.*

Baker, P. R. (2021). *Handbook on Negotiating Sustainable Development Provisions in Preferential Trade Agreements.* Retrieved from UNESCAP: *https://repository.unescap.org/bitstream/handle/20.500.12870/4285/ESCAP-2021-MN-Handbook-negotiating-sustainable-development.pdf?sequence=1&isAllowed=y*

Baker, P. R., Le, L., Vanzetti, D., & Ngov, P. (2022). *Handbook on Trade Analysis.* Sept: GIZ.

Baker, P., & Le, L. (2022). *Digital Trade under CPTPP and its implications for the UK.* Retrieved from UK Parliament: *https://committees.parliament.uk/writtenevidence/110995/pdf/*

Baker, P., & Le, L. (2022). *Guidebook on Trade Impact Assessments.* Retrieved from www.unctad.org: *https://unctad.org/system/files/official-document/ditctncd2021d4_en.pdf*

Banga, K., Macleod, J., & Mendez-Parra, M. (2021). *Digital trade provisions in the AfCFTA: What can we learn from South–South trade agreements?* Retrieved from *https://set.odi.org/wp-content/uploads/2021/04/Digital-trade-provisions-in-the-AfCFTA.pdf*

Berka, W. (2017). CETA, TTIP, TiSA, and Data Protection. In S. Griller, W. Obwexer, & E. Vranes, *Mega-Regional Trade Agreements: CETA, TTIP, and TiSA: New Orientations for EU External Economic Relations.* Oxford. Retrieved from *https://academic.oup.com/book/26602/chapter/195266134*

Borne, K. (2021, July 6). *Top 10 Data Innovation Trends During 2020*. Retrieved from Rocket-Powered Data Science: *http://rocketdatascience.org/?p=1589*

Bossmann, J. (2016, October 21). *Top 9 ethical issues in artificial intelligence*. Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/?*

Bracy, J. (2023, March 8). UK introduces draft data protection reform. *International Association of Privacy Professionals*.

Bryant, J. (2021, May 25). Three years in, GDPR highlights privacy in global landscape. *International Association of Privacy Professionals*.

Bukht, R., & Heeks, R. (2017). *Defining, Conceptualising and Measuring the Digital Economy.* Development Informatics Working Paper no. 68. Retrieved from *https://ssrn.com/abstract=3431732 or http://dx.doi.org/10.2139/ssrn.3431732*

Burri, M. (2017). The Regulation of Data Flows Through Trade Agreements. *Georgetown Journal of International Law, Vol. 48, No. 1, 2017*. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3028137*

Burri, M. (2021). *Big Data and Global Trade Law.* Cambridge: Cambridge University Press.

Burri, M., Callo-Müller, M. V., & Kugler, K. (2022). *TAPED: Trade Agreement Provisions on Electronic Commerce and Data*. Retrieved from *https://unilu.ch/taped*

Castro, D., & Korte, T. (2013, November 3). *Data Innovation 101*. Retrieved from Center for Data Innovation: *https://datainnovation.org/2013/11/data-innovation-101/*

Chenaoui, H. (2018, September 11). Moroccan data protection law: Moving to align with EU data protection? *International Association of Privacy Professionals*.

CIGI. (2018). *Data Governance in the Digital Age.* Centre for International Governance Innovation. Retrieved from *https://www.cigionline.org/static/documents/documents/Data%20Series%20Special%20Reportweb.pdf*

Ciuriak, D. (2018). *The Economics of Data: Implications for the Data-Driven Economy.* Centre for International Governance Innovation.

CloudSufi. (2021, November 16). *https://www.cloudsufi.com/why-is-data-the-backbone-of-the-digital-economy/*. Retrieved from CloudSufi: *https://www.cloudsufi.com/why-is-data-the-backbone-of-the-digital-economy/*

Cory, N. (2017, May 1). *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* Retrieved from Information Technology & Innovation Foundation: *https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/*

Cory, N., & Dascoli, L. (2021, July 19). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. *Information Technology and Information Foundation*.

Crocetti, P., Peterson, S., & Hefner, K. (n.d.). *What is data protection and why is it important?* Retrieved from *https://www.techtarget.com/searchdatabackup/definition/data-protection*

Daigle, B. (2021). Data Protection Laws in Africa: A Pan-African Survey and Noted Trends. *Journal of International Commerce and Economics*.

data.gov.uk. (n.d.). *data.gov.uk*. Retrieved from *https://www.data.gov.uk/*

de la Cruz, R., & Hau, S. (2022, March). *UK: Requirements for international data transfers under UK and EU data protection regimes.* Retrieved from Data Guidance: *https://www.dataguidance.com/opinion/uk-requirements-international-data-transfers-under*

DLA Piper. (2023). Retrieved from *https://www.dlapiperdataprotection.com/*

DLA Piper. (2023, January 29). *Data Protection Laws around the World - United States*. Retrieved from *https://www.dlapiperdataprotection.com/index.html?t=law&c=US*

Dür, A., Baccini, L., & Elsig, M. (2022). *The Design of International Trade Agreements: Introducing a New Database.* Retrieved from *https://www.designoftradeagreements.org/*

European Commission. (2016, April). *Handbook for Trade Sustainability Impact Assessment.* Retrieved from trade.ec.europa.eu: *https://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154464.PDF*

European Commission. (2023, March 24). *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data*. Retrieved from European Commission: *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data*

European Commission. (n.d.). *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection.* Retrieved from European Commission: *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*

European Commission. (n.d.). *Shaping Europe's digital future: Free flow of non-personal data*. Retrieved from *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data#:~:text=The%20Regulation%20on%20the%20free,and%20IT%20systems%20in%20Europe*.

European Parliament. (2016, January 25). *Report 25 January 2016 Containing the European Parliament's Recommendations to the Commission on the Negotiations for the Trade in Services Agreement (TiSA)' (2015/2233(INI), [A8-0009/2016])*. Retrieved from *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0009+0+DOC+XML+V0//EN*

Gao, H. (2022, January 18). Data sovereignty and trade agreements: Three digital kingdoms. *Hinrich Foundation*.

Gawen, E., Hirschfeld, A., Kenny, A., Stewart, J., & Middleton, E. (2021). *Open source in government: creating the conditions for success.* London: Public Digital. Retrieved from *https://assets.public.digital/Open_Source_Report.pdf*

GDPR.EU. (n.d.). *hat is GDPR, the EU's new data protection law?* Retrieved from GDPR.EU: *https://gdpr.eu/what-is-gdpr/*

Giddings, A., Islam, E., Kao, K., & Kopp, E. (2021). *Towards a Global Approach to Data in the Digital Age.* IMF. Retrieved from *https://www.elibrary.imf.org/view/journals/006/2021/005/article-A001-en.xml*

Githaiga, J., & Kurji, J. A. (2023, February 6). *Kenya: Data Privacy Comparative Guide*. Retrieved from Mondaq: *https://www.mondaq.com/privacy/1190020/data-privacy-comparative-guide*

González, J. L., Casalini, F., & Porras, J. (2022). *A Preliminary Mapping of Data Localisation Measures.* OECD Publishing.

Google & IFC. (2020). *e-Conomy Africa 2020 - Africa's $180 Billion Internet Economy Future.* Retrieved from *https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/google-e-conomy*

GovTech Singapore. (2018, October 03). *ABCD: not as easy as you might think*. Retrieved from GovTech Singapore: *https://www.tech.gov.sg/media/technews/stack-18-abcd-ot-as-easy-as-you-might-think*

Greenberg, B. A. (2016). Rethinking Technology Neutrality. *Minnesota Law Review. 207*. Retrieved from *https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1206&context=mlr*

Greenleaf, G. (2018). Looming Free Trade Agreements Pose Threats to Privacy. 152 Privacy Laws & Business International Report. *152 Privacy Laws & Business International Report*, 23-27. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3199889*

Greenleaf, G., & Cottier, B. (2022). International and regional commitments in African data privacy laws: A comparative analysis. *Computer Law & Security Review, 44*.

GSMA. (2022). *The State of Mobile Internet Connectivity Report 2022.* Retrieved from *https://www.gsma.com/r/somic/*

GSMA. (2023). *The Mobile Economy 2023.* Retrieved from *https://www.gsma.com/mobileeconomy/wp-content/uploads/2023/03/270223-The-Mobile-Economy-2023.pdf*

Gurin, J. (2014). Big Data and Open Data: How open will the future be? *Journal of Law and Policy for the Information Society Vol 10:3*, 691-704. Retrieved from *https://core.ac.uk/download/pdf/159607722.pdf*

Gurin, J. (2014, April 15). *Big data and open data: what's what and why does it matter?* Retrieved from The Guardian: *https://www.theguardian.com/public-leaders-network/2014/apr/15/big-data-open-data-transform-government*

Hagiu, A., & Wright, J. (2020, February). *When Data Creates Competitive Advantage and When It Doesn't*. Retrieved from Harvard Business Review: *https://hbr.org/2020/01/when-data-creates-competitive-advantage*

Harvard Business Review. (2021). Customer Data: Designing for Transparency and Trust. *Harvard Business Review*.

Hinrich Foundation. (2019, February 21). Data localisation and other barriers to digital trade.

HM Government. (2013). *Open Data White Paper. Unleashing the Potential.* Retrieved from *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf*

Huawei & Oxford Economics. (2017). *Digital Spillover. Measuring the true impact of the digital economy.* Retrieved from *https://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf*

Hulme, M. H. (2016). Preamble in Treaty Interpretation. *University of Pennsylvania Law Review Vol 164*, 1281-1343. Retrieved from *https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9527&context=penn_law_review&httpsredir=1&referer=*

IBM. (n.d.). *What is artificial intelligence?* Retrieved from IBM: *https://www.ibm.com/topics/artificial-intelligence*

IBM. (n.d.). *What is machine learning?* Retrieved from IBM: *https://www.ibm.com/topics/machine-learning*

ICC. (2022). *ICC White Paper on Delivering Universal Meaningful Connectivity.* Retrieved from *https://iccwbo.org/wp-content/uploads/sites/3/2022/05/2022-icc-white-paper-delivering-connectivity.pdf*

IIF. (2020). *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy.* Institute of International Finance. Retrieved from *https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf*

ITU. (2013). *HIPSSA –Data Protection: SADC Model Law.*

ITU. (2021). *Measuring digital development Facts and Figures 2021.* Retrieved from *https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf*

ITU. (2022). *Measuring digital development: Facts and Figures 2022.* International Telecommunication Union. Retrieved from *https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2022-pdf-e.pdf*

Kanwar, S., Reddy, A., Kedia, M., & Manish, M. (2022). *The Emerging Era of Digital Identities: Challenges and Opportunities for the G20.* ADBI Institute. Retrieved from *https://www.adb.org/sites/default/files/publication/822681/adbi-brief-emerging-era-digital-identities-challenges-and-opportunities-g20.pdf*

Kennedy, G., & Lee, K. H. (2021). *Finding Harmony - ASEAN Model Contractual Clauses and Data Management Framework Launched.* Retrieved from *https://www.lexology.com/library/detail.aspx?g=be41251e-f5f0-4062-a02b-5bffbb8f16ad*

Koigi, B. (2020, 08 10). *Africa data centre market to reach $3 billion by 2025.* Retrieved from Africa Tech: *https://africabusinesscommunities.com/tech/tech-news/africa-data-center-market-to-reach-$3-billion-by-2025-report/*

Kudo, F., & Soble, J. (2022, May 20). *Every country has its own digital laws. How can we get data flowing freely between them?* Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/*

Kuo, M. (2022, September 26). Trafficking Data: China's Pursuit of Digital Sovereignty: Insights from Aynne Kokas. *The Diplomat*.

Mattoo, A., & Schuknecht, L. (1999). *Trade Policies for Electronic Commerce.* World Bank. Retrieved from *https://elibrary.worldbank.org/doi/10.1596/1813-9450-2380*

Mbengue, M. M. (2006, September). *Preamble.* Retrieved from Oxford Public International Law: *https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1456*

McKinsey. (2013, October 1). *Open data: Unlocking innovation and performance with liquid information*. Retrieved from *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information*

McKinsey. (2022, June 30). *Localisation of data privacy regulations creates competitive opportunities*. Retrieved from McKinsey: *https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities*

McKinsey. (2022, August 17). *What is the Internet of Things?* Retrieved from McKinsey: *https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-internet-of-things*

Meddin, E. (2020). The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and Article XVII of the General Agreement on Trade in Services. *American University International Law Review, 35*(4).

Mitchell, A. D., & Hepburn, J. (2017). Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. *19 Yale Journal of Law and Technology 182 (2017)*, 182-237. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2846830*

Mittelstadt, B. (2021). *The impact of Artificial Intelligence on the Doctor-Patent Relationship.* Council of Europe. Retrieved from *https://rm.coe.int/inf-2022-5-report-impact-of-ai-on-doctor-patient-relations-e/1680a68859*

Nordhaug, L. M., & Harris, L. (2021). Digital public goods: Enablers of digital sovereignty. In OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation.* Retrieved from *https://www.oecd-ilibrary.org/sites/c023cb2e-en/index.html?itemId=/content/component/c023cb2e-en*

OAG California. (2023, April 24). *California Consumer Privacy Act (CCPA)*. Retrieved from Office of the Attorney General - State of California Department of Justice: *https://oag.ca.gov/privacy/ccpa*

OECD. (2011). *OECD Guide to Measuring the Information Society 2011.*

OECD. (2013). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*

OECD. (2013). *The OECD Privacy Framework.* Retrieved from *https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*

OECD. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being.* Paris: OECD Publishing.

OECD. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being.* Paris: OECD Publishing.

OECD. (2020). *OECD Open, Useful and Re-usable Data (OURdata) Index: 2019.*

OECD. (2022). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188.* Retrieved from *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*

OECD. (n.d.). *Data-driven innovation for growth and well-being*. Retrieved from OECD: *https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm*

OECD. (n.d.). *Digital trade*. Retrieved from Organisation for Economic Co-operation and Development: *https://www.oecd.org/trade/topics/digital-trade/*

OECD. (n.d.). *Why data governance matters*. Retrieved from Organisation for Economic Cooperation and Development: *https://search.oecd.org/digital/data-governance/*

OECD. (n.d.). *Personal Data Protection at the OECD*. Retrieved from *https://www.oecd.org/general/data-protection.htm*

OECD, WTO & IMF. (2020). *Handbook on Measuring Digital Trade.* Retrieved from *https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf*

Okwara, E. (2022, September 27). A privacy pro's odyssey in Africa. *International Association of Privacy Professionals*.

One Trust Data Guidance. (2022, December 22). *Morocco: CNDP reminds controllers of data breach procedure*. Retrieved from Data Guidance: *https://www.dataguidance.com/news/morocco-cndp-reminds-controllers-data-breach-procedure*

One Trust Data Guidance. (n.d.). *Morocco*. Retrieved from Data Guidance: *https://www.dataguidance.com/jurisdiction/morocco*

OneTrust. (2022, September 16). *ECOWAS Act on Personal Data Protection*. Retrieved from OneTrust DataGuidance: *https://www.dataguidance.com/opinion/african-bodies-ecowas-act-personal-data-protection*

Onuoha, R. (2022, November 29). *Africa's Leading Lights: Regional Network Readiness for Digital Transformation*. Retrieved from Portulans Institute: *https://portulansinstitute.org/africas-leading-lights/*

Open Data Handbook. (2023). *The Open Data Handbook*. Retrieved from *https://opendatahandbook.org/guide/en/*

POPIA. (n.d.). *POPIA*. Retrieved from POPIA: *https://popia.co.za/*

Redman, T. C. (2015, May 20). *4 Business Models for the Data Age*. Retrieved from Harvard Business Review: *https://hbr.org/2015/05/4-business-models-for-the-data-age*

Research and Markets. (2022). *Africa Data Center Market - Industry Outlook & Forecast 2022-2027.*

Rotella, P. (2012, April 2). *Is Data The New Oil?* Retrieved from Forbes: *https://www.forbes.com/sites/perryrotella/*

SADC. (2021). *Selection of Individual Consultant: Consultancy for Revision and Modernisation of the SADC Data Protection Model Law.*

Sadowski, J. (2016, August 31). *Companies Are Making Money from Our Personal Data, but at What Cost?* Retrieved from The Guardian: *https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon*

Satariano, A. (2018, May 6). *What the G.D.P.R., Europe's Tough New Data Law, Means for You*. Retrieved from The New York Times: *https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html*

Schalkwyk, F. v., Willmers, M., & Schonwetter, T. (2015). *Embedding Open Data Practice: Developing Indicators on the Institutionalisation of Open Data Practices in two African Government.* World Wide Web Foundation. Retrieved from *http://webfoundation.org/docs/2015/08/ODDC-2-Embedding-Open-Data-Practice-FINAL.pdf*

Schenker, C. (2015). *Practice Guide to International Treaties.* Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera .

Simmons, D. (2022, January 13). *17 Countries with GDPR-like Data Privacy Laws*. Retrieved from Comforte: *https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws*

Smart Africa Alliance. (2021). *Artificial Intelligence for Africa Blueprint.* Smart Africa Alliance. Retrieved from *https://smart.africa/board/login/uploads/70029-eng_ai-for-africa-blueprint.pdf*

Smart Africa Alliance. (2021). *Blueprint for e-Payments for the Facilitation of Digital Trade across Africa.* Retrieved from *https://smartafrica.org/knowledge/blueprint-for-e-payments-for-the-facilitation-of-digital-trade-across-africa/*

Stanford University. (2020). *Artificial Intelligence Definitions*. Retrieved from Stanford University Human-Centered Artificial Intelligence: *https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf*

Thirani, V., & Gupta, A. (2017, September 22). *The value of data*. Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2017/09/the-value-of-data/*

UK Parliament. (2023, March 8). *British Businesses to Save Billions Under New UK Version of GDPR*. Retrieved from *https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr*

UK Parliament. (2023, April 18). *Parliamentary Bills: Data Protection and Digital Information (No. 2) Bill*. Retrieved from *https://bills.parliament.uk/bills/3430*

UN Global Pulse. (n.d.). *UN Global Pulse Principles on Data Protection and Privacy*. Retrieved from UN Global Pulse: *https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/*

UNCTAD. (2012). *Harmonising Cyberlaws and Regulations: The Experience of the East African Community.* New York and Geneva: United Nations Conference on Trade and Development. Retrieved from *https://au.int/sites/default/files/newsevents/workingdocuments/27223-wd-harmonizing_cyberlaws_regulations_the_experience_of_eac1.pdf*

UNCTAD. (2016). *Data protection regulations and international data flow: Implications for trade and development.*

UNCTAD. (2018). *Trade Policy Frameworks for Developing Countries: A Manual of Best Practice.*

UNCTAD. (2019). *Digital Economy Report 2019. Value creation and capture: Implications for Developing Countries.* New York: United Nations Conference in Trade and Development. Retrieved from *https://unctad.org/system/files/official-document/der2019_en.pdf*

UNCTAD. (2021). *Covid-19 and E-Commerce. A Global view.* New York: United Nations. Retrieved from *https://unctad.org/system/files/official-document/dtlstict2020d13_en_0.pdf*

UNCTAD. (2021, December 14). *Data Protection and Privacy Legislation Worldwide*. Retrieved from *https://unctad.org/page/data-protection-and-privacy-legislation-worldwide*

UNCTAD. (2021). *Digital Economy Report 2021. Cross-border data flows and development: For whom the data flow.* Geneva: United Nations. Retrieved from *https://unctad.org/system/files/official-document/der2021_en.pdf*

UNCTAD. (2021). *Estimates of global e-commerce 2019 and preliminary assessment of COVID-19 impact on online retail 2020. UNCTAD Technical Notes on ICT for Development No. 18.* United Nations. Retrieved from *https://unctad.org/system/files/official-document/tn_unctad_ict4d18_en.pdf*

UNCTAD. (2021). *Global E-Commerce Jumps to $26.7 Trillion, Covid-19 Boosts Online Retail Sales*. Retrieved from UNCTAD: *https://unctad.org/press-material/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-retail-sales*

UNCTAD. (2023). *G20 Members' Regulations of Cross-Border Data Flows.* Geneva: United Nations. Retrieved from *https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf*

UNDG. (2017). *United Nations Sustainable Development Goals Guidance Note on Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection.* United Nations Development Group.

United Nations. (2018). *Personal Data Protection and Privacy Principles.* Retrieved from *https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf*

United Nations. (2023). *Digital Inclusion.* Retrieved from *https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Definition_Digital-Inclusion.pdf*

WEF. (2011). *Personal Data: The Emergence of a New Asset Class.* Geneva: World Economic Forum.

WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows.* World Economic Forum.

WEF. (2022, May 20). *Every country has its own digital laws. How can we get data flowing freely between them?* Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/*

WEF. (2023). *Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows.*

World Bank. (2019). *Starting an Open Data Initiative*. Retrieved from Open Data Toolkit: *http://opendatatoolkit.worldbank.org/en/starting.html*

World Bank. (2021, May 13). *http://opendatatoolkit.worldbank.org/en/starting.html*. Retrieved from Open Data Toolkit: *http://opendatatoolkit.worldbank.org/en/starting.html*

World Bank. (2021). *World Development Report 2021: Data for Better Lives.* Retrieved from *https://www.worldbank.org/en/publication/wdr2021*

World Bank. (2023). *Identification for Development (ID4D) Practitioner's Guide*. Retrieved from *https://id4d.worldbank.org/guide/*

World Bank. (n.d.). *Starting an Open Data Initiative*. Retrieved from *http://opendatatoolkit.worldbank.org/en/starting.html*

WTO. (1999). *Council for Trade in Services – Report of the Meeting Held on 14 and 15 December 1998 – Note by the Secretariat, Doc. S/C/M/32.*

WTO. (1999). *Work Programme on Electronic Commerce – Progress Report to the General Council – Adopted by the Council for Trade in Services on 19 July 1999, Doc. S/L/74, 27 July 1999.*

WTO. (2016). *GATS 3 Article XIV (DS reports).*

WTO. (2021). *WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore.*

WTO. (2023, March 30). *E-commerce negotiators advance work, discuss development and data issues*. Retrieved from World Trade Organisation: *https://www.wto.org/english/news_e/news23_e/jsec_30mar23_e.htm*

WTO. (n.d.). *Joint Initiative on E-commerce*. Retrieved from World Trade Organisation: *https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm*

WTO Plurilaterals. (n.d.). *Joint Statement Initiative on Electronic Commerce*. Retrieved from WTO Plurilaterals: *https://wtoplurilaterals.info/plural_initiative/e-commerce/*

Yayboke, E., & Ramos, C. G. (2021, July 23). The Real National Security Concerns over Data Localization. *CSIS*.

Zillner, S., & Neururer, S. (2016). Big Data in the Health Sector (Chapter 10). In J. M. Cavanillas, E. Curry, & W. Wahlster, *New Horizons for a Data-Driven Economy. A Roadmap for Usage and Exploitation of Big Data in Europe* (pp. 179-194). Springer Open.

ANNEXES

ANNEXE 1. GLOSSAIRE

Le monde du numérique étant encore en pleine évolution, il n'existe pas de définitions officielles des nombreux termes liés au commerce numérique et à l'économie numérique. Ainsi, les définitions suivantes visent à faciliter les échanges plutôt qu'à établir une interprétation fixe des termes.

L'expression **« Intelligence artificielle (IA) »** a été proposée par le professeur émérite de l'université Stanford John McCarthy en 1955, qui la décrit comme « la science et la mécanique de concevoir des machines intelligentes » (Stanford University, 2020). L'IA désigne une intelligence ayant pour origine les machines, contrairement à l'intelligence naturelle dont les humains et animaux peuvent faire preuve, et qui implique une forme de conscience et d'émotivité. À titre de technologie, l'IA est un domaine qui associe science informatique et ensembles de données rigoureux, avec pour objectif la résolution des problèmes. Elle englobe également les sous-domaines de l'apprentissage automatique et de l'apprentissage profond, qui sont fréquemment mentionnés en combinaison avec l'intelligence artificielle (IBM, n.d.).

La **gouvernance des données** fait référence à diverses modalités, notamment les dispositions techniques, politiques, réglementaires ou institutionnelles qui affectent les données ainsi que leur cycle (création, collecte, stockage, utilisation, protection, accès, partage et suppression) entre les domaines politiques et les frontières organisationnelles et nationales (OECD, n.d.). Même si la portée peut être interprétée au sens large, les questions centrales en matière de gouvernance des données se résument à quatre thèmes clés : qui possède les données et qu'impliquent ces droits en matière de données, qui est autorisé à collecter les données, les réglementations en matière d'agrégation des données ainsi que les règles de transfert des droits en matière de données (CIGI, 2018).

La **localisation des données** est utilisée pour faire référence aux exigences de stockage et/ou traitement des données au sein du territoire national (González, Casalini, & Porras, 2022). Certains vont plus loin en exigeant que l'ensemble des traitements et de l'utilisation dérivée des données demeure à l'intérieur des frontières nationales (IIF, 2020). Dans le contexte des accords commerciaux, la localisation des données tend à relever de la disposition « implantation des installations informatiques » qui nécessite « l'utilisation ou l'implantation d'installations informatiques au sein du territoire [d'une] Partie à titre de condition à la réalisation d'activités commerciales au sein de ce territoire ».

Propriété des données désigne à la fois la détention et la responsabilité de l'information (Zillner & Neururer, 2016). En d'autres termes, la propriété des données peut être interprétée comme une forme de propriété ou comme une forme de contrôle. Il est, malgré tout, difficile d'inscrire « propriété des données » dans les lois traditionnelles en matière de propriété. S'agissant d'actifs incorporels, les données impliquent typiquement une attribution complexe des différents droits aux différentes parties prenantes en matière de données, nécessitant « la capacité à accéder, créer, modifier, combiner, tirer profit, vendre ou éliminer des données, mais également le droit d'attribuer ces privilèges d'accès à d'autres » (OECD, 2015).

Souveraineté des données désigne une approche politique qui préconise l'assujettissement des données aux lois et réglementations du pays où elles sont générées. La demande de souveraineté des données est guidée par des questions relatives au contrôle et à la propriété des données, particulièrement dans le contexte du cloud computing et de la circulation transfrontalière des données (Gao, 2022). Voir aussi « souveraineté numérique ».

L'innovation fondée sur les données (DDI) désigne l'utilisation des données et analyses en vue de l'amélioration ou du développement de nouveaux produits, processus, méthodes organisationnelles et marchés (OECD, 2015). Elle est souvent associée à la génération et à l'utilisation d'importants volumes de données, communément appelés « mégadonnées », afin de développer de nouveaux processus, industries et produits, et de créer des avantages compétitifs importants (OECD, n.d.).

Le terme **économie numérique** existe depuis près de 30 ans, l'origine du terme étant généralement attribuée au livre de Don Tapscott publié en 1996 intitulé « The Digital Economy: Promise and Peril in the Age of Networked Intelligence ». Depuis, de nombreuses définitions présentant différentes approches ont émergé pour définir l'économie numérique (Bukht & Heeks, 2017). Une approche consiste à envisager l'économie numérique comme « cette part de production économique provenant exclusivement ou principalement des technologies numériques, avec un modèle commercial basé sur les biens et services numériques » (UNCTAD, 2019; Bukht & Heeks, 2017).

La souveraineté numérique désigne le pouvoir et l'autorité d'un gouvernement national à prendre librement des décisions qui affectent les citoyens et les entreprises dans le domaine numérique, avec une couverture importante englobant les données, les logiciels, les normes et protocoles, les infrastructures et les services publics (Gawen, Hirschfeld, Kenny, Stewart, & Middleton, 2021; Nordhaug & Harris, 2021)

Commerce numérique englobe l'ensemble des commerces qui sont numériquement commandés et/ou numériquement délivrés (OECD, WTO & IMF, 2020). L'OCDE précise en outre que le commerce numérique « englobe les transactions numériques liées aux échanges de biens et de services qui peuvent être fournis sous forme numérique ou physique, et qui impliquent des consommateurs, des entreprises et des pouvoirs publics » (OECD, n.d.)

Commerce électronique désigne la vente ou l'achat de biens et services, réalisée par le biais de réseaux informatiques et de moyens spécifiquement conçus aux fins de recevoir ou passer des commandes. Cette définition du commerce électronique englobe les commandes passées sur des pages web, sur l'extranet ou via un système d'échange de données informatisé (EDI), tout en excluant les commandes effectuées via les appels téléphoniques, la télécopie ou les messages électroniques saisis manuellement (OECD, 2011). Le texte de négociation consolidé de la déclaration conjointe sur l'initiative (JSI) de l'OMC daté de septembre 2021 propose que « [Commerce numérique / commerce électronique] désigne la production, la distribution, le marketing, la vente ou la livraison de biens et services par voie électronique ». Cette proposition apporte une définition plus large en comparaison de celle de l'OCDE, car elle couvre l'ensemble des transactions pour lesquelles au moins une étape de commerce est réalisée par voie électronique.

L'Internet des objets (IDO) décrit les objets physiques qui incorporent des capteurs et déclencheurs qui communiquent avec les systèmes informatiques par le biais de systèmes filaires ou sans fil, permettant au monde physique d'être numériquement surveillé ou même contrôlé (McKinsey, 2022).

Implantation des installations informatiques désigne les exigences en matière de réglementations nationales pour localiser les serveurs informatiques et dispositifs de stockage pour le traitement ou le stockage d'informations destinés à un usage commercial au sein du territoire national à titre de condition pour réaliser des activités commerciales sur ce territoire (article 4.4, APEN).

Apprentissage automatique, à titre de domaine d'étude, désigne le domaine d'étude portant sur la manière dont les agents informatiques peuvent améliorer leur perception, connaissance, raisonnement ou leurs actions sur la base de l'expérience ou des données. Pour cela, l'apprentissage automatique s'appuie sur la science informatique, les statistiques, la psychologie, la neuroscience, les sciences économiques et la théorie du contrôle (Stanford University, 2020). En termes d'application, l'apprentissage automatique est une branche de l'intelligence artificielle (IA) et de la science informatique qui se concentre sur l'utilisation des données et des algorithmes afin d'imiter la manière dont les humains apprennent, améliorant au fur et à mesure sa précision (IBM, n.d.).

Données ouvertes désigne les données numériques qui sont mises à disposition suivant les caractéristiques techniques et juridiques nécessaires leur permettant d'être librement utilisées, réutilisées et redistribuées (article 9.1, APEN).

Données à caractère personnel désigne toutes les informations liées à un individu identifié ou identifiable (OECD, 2022). Certains cadres utilisent un terme similaire : « informations personnelles », qui désigne les « informations, y compris les données, qui portent sur une personne physique identifiée ou identifiable » (article 1.3, APEN).

Protection des données à caractère personnel désigne le domaine du droit qui prévoit des mesures administratives ou techniques qui visent à protéger les individus de l'utilisation abusive des données qui les concernent et à leur accorder le droit d'accès aux données en vue du contrôle de leur exactitude et pertinence (OECD, 2013). On peut aussi parler de « lois sur la protection des données » ou de « lois sur la protection de la vie privée ».

.

ANNEXE 2. EXEMPLES DE CADRES INTERNATIONAUX LIÉS AUX LIGNES DIRECTRICES EN MATIÈRE DE DONNÉES

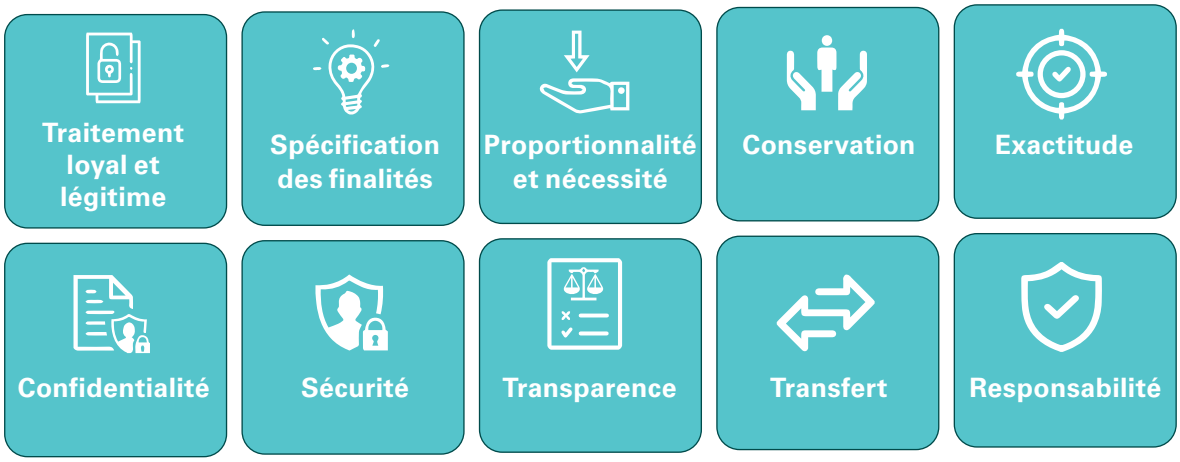
Quelques-uns des cadres internationaux les plus importants sont évoqués dans la présente annexe afin de déterminer les bonnes pratiques, tandis que certains cadres réglementaires nationaux sont également brièvement évoqués concernant la manière dont les juridictions traitent les problématiques liées aux données.

(I) PRINCIPES ET LIGNES DIRECTRICES DES NATIONS UNIES

Les Nations unies (ONU) ont mis au point une série de principes sur la confidentialité des données. Ils visent à promouvoir l'utilisation responsable des données pour le développement durable tout en préservant la vie privée et en protégeant les droits de l'homme (UN Global Pulse, n.d.). Ceux-ci comprennent les principes des Nations unies relatifs à la protection des données à caractère personnel et de la vie privée de 2018 (les « Principes ») ainsi que la Note d'orientation des Nations unies concernant les mégadonnées à l'appui de la réalisation de l'Agenda 2030 : confidentialité des données, éthique et protection (la « Note d'orientation »).

Les Principes, composés de 10 règles, établissent un cadre de base pour le traitement des « données à caractère personnel » par ou pour le compte des organisations du système des Nations unies, afin qu'elles s'acquittent des fonctions qui leur ont été attribuées. Objectifs de ces Principes : i) harmoniser les normes de protection des données à caractère personnel dans le système des Nations unies ; ii) faciliter le traitement responsable de données à caractère personnel ; et iii) garantir le respect des droits de l'homme et des libertés fondamentales des individus, en particulier le droit à la vie privée. Ces Principes peuvent aussi servir de référence pour le traitement de données à caractère non personnel (United Nations, 2018).

Illustration 10. Dix Principes des Nations unies relatifs à la protection des données à caractère personnel et de la vie privée



Source: (United Nations, 2018)

La Note d'orientation est centrée autour de neuf principes (**Error! Reference source not found.**) qui visent à soutenir les membres et partenaires du Groupe des Nations unies pour le développement, afin d'établir un cadre efficace et cohérent en matière de confidentialité, de protection des données et d'éthique des données pour le Groupe des Nations unies pour le développement (UNDG) concernant l'utilisation des mégadonnées. Il convient de noter que cette Note d'orientation ne constitue pas un document juridique, mais sert uniquement de base minimale en matière d'autoréglementation qui peut être développée et abordée plus en détail par les organisations chargées de l'exécution (UNDG, 2017). Au vu de leur périmètre élargi, les principes de la Note d'orientation liés aux données fournissent également des indications plus détaillées sur les normes attendues en matière de traitement et d'utilisation des données, ainsi que concernant la gestion du risque et le contrôle de la qualité des données. Les Principes sont résumés dans l'Annex 4.

Illustration 11. Neuf principes de la Note d'orientation des Nations unies concernant les mégadonnées

(II) LES LIGNES DIRECTRICES DE L'OCDE EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

Les lignes directrices de l'Organisation de développement et de coopération économiques (OCDE) régissant la protection de la vie privée constituent également un cadre international important pour la protection des données. Les lignes directrices de l'OCDE régissant la protection de la vie privée ont initialement été adoptées en 1980 pour orienter le traitement responsable des données à caractère personnel. Depuis lors, elles ont été mises à jour et révisées afin de se conformer à l'évolution rapide de l'environnement de la confidentialité des données (OECD, n.d.). Les lignes directrices de l'OCDE régissant la protection de la vie privée reposent sur certains principes fondamentaux ayant trait à l'importance de la qualité des données, aux spécifications des finalités, à la responsabilité et aux droits individuels (OECD, 2013). Parmi d'autres obligations, les principes nécessitent ainsi des organisations qu'elles obtiennent le consentement des individus avant la collecte ou l'utilisation de leurs données à caractère personnel et que des mesures appropriées soient mises en place afin de protéger les données à caractère personnel d'un accès ou d'une utilisation non autorisés (OECD, 2013).

L'une des caractéristiques clés des lignes directrices de l'OCDE régissant la protection de la vie privée est l'accent qu'elles mettent sur la circulation transfrontalière des données. Les lignes directrices de l'OCDE régissant la protection de la vie privée insistent sur l'importance d'adopter des lois exhaustives sur la protection des données. Celles-ci doivent inclure des dispositions sur les transferts transfrontaliers de données, qui doivent être assorties de mesures de protection appropriées. En outre, ces lignes directrices spécifient que toute restriction imposée à la circulation transfrontalière de données doit être proportionnelle aux risques (OECD, 2013). Les lignes directrices insistent également sur l'importance de la coopération internationale et de l'interopérabilité.

(III) CADRE DE PROTECTION DE LA VIE PRIVÉE DE L'APEC ET SYSTÈME DE RÈGLES DE CONFIDENTIALITÉ TRANSFRONTALIÈRES (CBPR) DE L'APEC

Parmi les initiatives bien établies visant à promouvoir les normes internationales en matière d'élaboration des règles liées à la gouvernance des données, on trouve le cadre de protection de la vie privée de l'APEC, le système de règles de confidentialité transfrontalières (CBPR) de l'APEC et le cadre de gestion des données (DMF) ainsi que les clauses contractuelles types (CCT) pour la circulation transfrontalière des données de l'Association des nations de l'Asie du Sud-Est (ANASE).

- Le Cadre de protection de la vie privée de l'APEC fournit des principes sur la collecte, la détention, le traitement, l'utilisation, le transfert ou la divulgation d'informations personnelles appliquées à des personnes ou organisations des secteurs public et privé qui contrôlent chacun des processus susmentionnés. Ce Cadre favorise une approche flexible de la protection de la confidentialité des informations parmi les économies membres de l'APEC, en évitant la création d'obstacles inutiles pour la circulation des données (APEC, 2005).
- Le système des Règles de confidentialité transfrontalières de l'APEC (CBPR) constitue une certification sur la confidentialité des données soutenue par le gouvernement. Les entreprises peuvent y adhérer pour prouver qu'elles se conforment aux dispositifs de protection de la confidentialité des données reconnus à l'échelle internationale (APEC, 2019). Le système CBPR requiert des entreprises participantes qu'elles conçoivent et mettent en œuvre des politiques de confidentialité des données conformes au Cadre de protection de la vie privée de l'APEC.

- Le DMF de l'ANASE vise à apporter une orientation pratique à l'ensemble des entreprises du secteur privé en matière de mise en œuvre d'un système de gestion des données basé sur les bonnes pratiques et les principes fondamentaux de gestion, en utilisant une méthodologie basée sur les risques.
- Les CCT sont des clauses contractuelles standard recommandées dans les accords liés au transfert transfrontalier des données à caractère personnel au sein de la région. Elles visent à synthétiser les obligations clés en matière de protection des données et à réduire les coûts de négociation et de conformité (Kennedy & Lee, 2021).

Même si l'ensemble de ces initiatives sont loin d'atteindre toute leur ampleur et leur impact, elles constituent des exemples de bonnes pratiques dans le cadre du développement de normes régionales et internationales de gouvernance des données en faveur d'une économie numérique ouverte.

(IV) INITIATIVE DE LIBRE CIRCULATION DES DONNÉES EN TOUTE CONFIANCE

De la même façon, une initiative plus récente – la libre circulation des données en toute confiance (DFTT) du Forum économique mondial (FEM) – vise à faciliter le libre flux des données en garantissant la confidentialité et la sécurité des données. Lancée par l'ancien premier ministre japonais Abe Shinzo en 2019, l'initiative de libre circulation des données en toute confiance (DFFT) de la FEM est fondée sur le postulat que la libre circulation des données est essentielle à la croissance économique et à l'innovation, et que la protection et la confidentialité des données sont capitales au maintien de la confiance dans l'économie numérique (WEF, 2020). De ce fait, l'initiative tend à trouver un équilibre entre la promotion de la libre circulation des données et la protection des informations personnelles.

Les principes soulignés dans l'initiative de libre circulation des données en toute confiance de la FEM visent à fournir un cadre aux décideurs politiques et leaders du marché, qui leur permettra de développer des cadres réglementaires favorables (WEF, 2022). Une feuille de route pour la coopération a été adoptée en 2021, avec notamment pour priorités quatre domaines de coopération : localisation des données, coopération réglementaire, accès des gouvernements aux données et partage des données pour des secteurs prioritaires (Arasasingham & Goodman, 2023). Un plan d'action a en outre été imaginé en 2022. Il étend la coopération en matière de future interopérabilité réglementaire numérique ainsi que le partage de connaissance sur les espaces de données internationaux (Arasasingham & Goodman, 2023). Étant donné sa portée internationale et l'accent mis sur le secteur privé, l'initiative pourrait contribuer à réduire la fragmentation des exigences réglementaires à l'échelle internationale, ce qui simplifierait l'accessibilité des entreprises aux données et leur utilisation au-delà des frontières. Malgré tout, une réserve courante liée à l'initiative ainsi qu'aux autres cadres évoqués est qu'il est difficile pour les pays de développer un cadre réglementaire commun, car les différentes juridictions disposent de différents cadres juridiques et réglementaires et de différentes ententes liées à la protection des données et de la vie privée qui rendent difficile l'élaboration de lignes directrices et d'un ensemble de principes communs pouvant s'appliquer partout (WEF, 2023).

Le RGPD de l'UE est un règlement exhaustif et rigoureux sur la protection des données. En raison de sa portée, le RGPD a servi d'inspiration à quantité de réglementations dans le monde entier. On compte notamment la Loi brésilienne générale sur la protection des données à caractère personnel, les Lois de Virginie et Californie sur la protection des données, ainsi que la Loi sur la protection des données à caractère personnel proposée en Inde (Bryant,

2021). Parmi les dispositions distinctives du RGPD de l'UE qui ont valu à la loi sa réputation, on peut citer :

- **Application extra-territoriale :** Le RGPD de l'UE a été adopté par l'UE, mais il s'applique à toute entité qui traite ou collecte des données portant sur des sujets de l'UE, que l'entité se trouve dans l'UE ou non (GDPR.EU, n.d.).
- **Consentement :** Lors du traitement, de la collecte ou de l'utilisation des informations personnelles dans l'UE, le RGPD exige de l'ensemble des entités qu'elles obtiennent le consentement explicite des individus concernés. En outre, les personnes concernées ont la possibilité de retirer leur consentement à tout moment.
- **Droits des personnes concernées :** Le RGPD reconnaît de nombreux droits en matière de vie privée aux personnes concernées, leur accordant un contrôle plus important sur les données les concernant qui pourraient être collectées, enregistrées et traitées par des organisations.
- **Application et sanctions :** Le non-respect du RGPD peut entraîner des pénalités pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel, le chiffre le plus élevé étant retenu.

Le RGPD de l'UE impose aussi certaines restrictions sur la circulation transfrontalière des données à caractère personnel. Suivant les dispositions du RGPD, le transfert de données à caractère personnel vers des pays présentant un niveau de protection approprié est garanti dans le cadre de la législation nationale. La Commission européenne est chargée de définir l'adéquation du niveau de protection des données dans les pays non membres de l'UE. Seuls quelques pays sont reconnus comme disposant de réglementations adéquates (European Commission, n.d.).[80] En l'absence de cette adéquation, des organisations recourent à d'autres mécanismes légaux pour transférer des données à caractère personnel hors de l'UE. Ceux-ci peuvent comprendre des clauses contractuelles types, des règles d'entreprise contraignantes, des codes de conduite et des dispositifs de certification (Commission européenne, n.d.).

L'UE a également adopté une législation à l'égard de la circulation des données à caractère non personnel. L'un des objectifs de l'UE est de faciliter la circulation des données en Europe, permettant aux organisations et aux pouvoirs publics de collecter et gérer les données à caractère non personnel vers l'emplacement de leur choix au sein du bloc (European Commission, n.d.). La réglementation d'un cadre pour la libre circulation des données à caractère non personnel vise ainsi à éliminer les obstacles qui entravent la libre circulation des données à caractère non personnel entre différents pays de l'UE. La réglementation vient compléter le RGPD et garantit une approche uniforme et cohérente de la libre circulation de l'ensemble des données au sein de l'UE. On trouve parmi certaines des obligations clés qui résultent de la réglementation la disponibilité des données aux fins du contrôle réglementaire, la portabilité des données entre fournisseurs de services cloud pour les utilisateurs professionnels, ainsi qu'une meilleure uniformité et cohérence en matière de préoccupations liées à la sécurité (European Commission, n.d.).

80 Les pays reconnus par la Commission de l'UE comme disposant de règlements adéquats sur la protection des données incluent Andorre, l'Argentine, le Canada (organisations commerciales), les îles Féroé, Guernesey, Israël, l'Île de Man, le Japon, Jersey, la Nouvelle-Zélande, la République de Corée, la Suisse, le Royaume-Uni et l'Uruguay.

ANNEXE 3. PRINCIPES DES NATIONS UNIES RELATIFS À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET DE LA VIE PRIVÉE

1. TRAITEMENT LOYAL ET LÉGITIME

Les organisations du système des Nations unies doivent traiter les données à caractère personnel de manière loyale, conformément à leurs mandats et instruments de gouvernance et sur la base de l'un des points suivants : i) le consentement de la personne concernée ; ii) les meilleurs intérêts de la personne concernée, conformément aux mandats des organisations du système des Nations unies concernées ; iii) les mandats et instruments de gouvernance des organisations du système des Nations unies concernées ; ou iv) n'importe quelle autre base juridique spécifiquement identifiée par les organisations du système des Nations unies concernées.

2. SPÉCIFICATION DES FINALITÉS

Les données à caractère personnel ne doivent être traitées qu'à des fins explicites, en cohérence avec les mandats des organisations du système des Nations unies concernées, et prendre en compte l'équilibre des droits, libertés et intérêts qui conviennent. Les données à caractère personnel ne doivent pas être traitées d'une manière qui puisse être incompatible avec les finalités en question.

3. PROPORTIONNALITÉ ET NÉCESSITÉ

Le traitement des données à caractère personnel doit être pertinent, limité et adéquat à ce qui est nécessaire en lien avec les finalités spécifiées du traitement des données à caractère personnel.

4. CONSERVATION

Les données à caractère personnel ne doivent être conservées que pendant la durée nécessaire dans le cadre des finalités spécifiées.

5. EXACTITUDE

Les données à caractère personnel doivent être exactes et, le cas échéant, actualisées afin de répondre aux finalités spécifiées.

6. CONFIDENTIALITÉ

Les données à caractère personnel doivent être traitées dans le strict respect de la confidentialité.

7. SÉCURITÉ

Des mesures de protection et procédures techniques, physiques, administratives et organisationnelles appropriées doivent être mises en place afin de protéger la sécurité des données à caractère personnel, notamment contre l'accès non autorisé ou accidentel, les dommages, les pertes ou autres risques posés par le traitement des données.

8. TRANSPARENCE

Le traitement des données à caractère personnel doit être réalisé avec transparence par rapport aux personnes concernées, le cas échéant, et à chaque fois que cela est possible. On devrait par exemple compter la communication d'informations concernant le traitement de leurs données à caractère personnel ainsi que sur la manière d'effectuer une demande d'accès, la vérification, la rectification et/ou la suppression de ces données à caractère personnel, dans la mesure où les finalités spécifiées pour lesquelles les données à caractère personnel sont traitées ne sont pas vouées à l'échec.

9. TRANSFERTS

Au cours de l'acquittement des fonctions qui lui ont été attribuées, une organisation du système des Nations unies a la possibilité de transférer des données à caractère personnel à un tiers, à condition que, dans ces circonstances, l'organisation du système des Nations unies s'assure que le tiers procure un niveau approprié de protection pour les données à caractère personnel en question.

10. RESPONSABILITÉ

Les organisations du système des Nations unies doivent disposer de politiques et mécanismes adéquats afin de pouvoir adhérer à ces principes.

ANNEXE 4. NOTE D'ORIENTATION DES NATIONS UNIES CONCERNANT LES MÉGADONNÉES : PRINCIPES CLÉS

1. UTILISATION LICITE, LÉGITIME ET LOYALE

Que ce soit directement ou par le biais d'un contrat passé avec un fournisseur de données tiers, les données doivent être collectées et utilisées par des moyens licites, légitimes et loyaux. L'accès aux données, leur analyse et toute autre utilisation qui leur est réservée devront être conformes aux lois applicables, y compris les lois sur la confidentialité et la protection des données, ainsi qu'aux normes de confidentialité et de conduite morale et éthique les plus rigoureuses. L'accent est également mis sur le consentement adéquat de la personne dont les données sont utilisées. L'accès aux données, leur analyse et toute autre utilisation qui leur est réservée devront toujours tenir compte des intérêts légitimes des personnes dont les données sont utilisées afin de garantir une utilisation loyale des données. Les données ne devront pas être utilisées d'une manière qui porte atteinte aux droits de l'homme ou de toute autre manière susceptible d'avoir des effets injustifiés ou néfastes. En conséquence, il est recommandé de toujours évaluer la légitimité et la loyauté de l'utilisation des données en prenant en compte les risques, les préjudices et les avantages.

2. SPÉCIFICATION DES FINALITÉS, LIMITATION DE L'UTILISATION, COMPATIBILITÉ AVEC LES FINALITÉS

L'utilisation de données doit être cohérente par rapport aux finalités pour lesquelles les données ont été obtenues. La finalité ne peut être changée à moins que ce ne soit sur une base légitime. En outre, la finalité doit être légitime et formulée d'une manière aussi concise et précise que possible. Par ailleurs, la finalité de l'accès ou de la collecte de données doit être clairement formulée au moment de l'accès ou de la collecte.

3. ATTÉNUATION DES RISQUES ET ÉVALUATION DES RISQUES, DES PRÉJUDICES ET DES AVANTAGES

Les données devront être collectées et utilisées conformément aux lois applicables, en respectant la vie privée des individus et en protégeant leurs droits. L'utilisation des données sensibles doit impliquer la consultation des groupes concernés ou de leurs représentants afin d'atténuer les risques associés. Les risques et préjudices potentiels ne devront pas être excessifs par rapport aux avantages de l'utilisation des données.

4. DONNÉES SENSIBLES ET CONTEXTES SENSIBLES

Au cours de la collecte, de l'accès ou de l'analyse des données concernant des groupes vulnérables ou de données sensibles, des normes plus strictes de protection des données devront être appliquées. En outre, il est important d'envisager la possibilité que le contexte d'utilisation puisse transformer des données non sensibles en données sensibles, par exemple les facteurs culturels ou politiques, et de prendre en compte la manière dont cela affecte des individus ou groupes d'individus.

5. SÉCURITÉ DES DONNÉES

Des mesures et procédures techniques et organisationnelles rigoureuses de protection devront être mises en place afin de garantir une gestion adéquate des données et d'empêcher toute utilisation ou divulgation non autorisée de données à caractère personnel. Des technologies renforçant la protection de la vie privée devront être utilisées à tous les stades du cycle de vie des données. De plus, le cas échéant, les données à caractère personnel devront être anonymisées afin de réduire les risques de violation de la vie privée.

6. CONSERVATION ET MINIMISATION DES DONNÉES

L'accès aux données, leur analyse et toute autre utilisation qui leur est réservée devront être limités au minimum nécessaire pour atteindre la finalité pour laquelle les données sont traitées. De plus, la quantité de données collectées devra également être limitée au minimum nécessaire. L'utilisation des données devra être contrôlée afin de veiller à ce que les précédents points soient respectés. En outre, suite à l'utilisation des données, celles-ci devront être supprimées définitivement, à moins que leur conservation ne soit justifiée.

7. QUALITÉ DES DONNÉES

Les données devront être contrôlées du point de vue de leur exactitude, pertinence, intégrité, exhaustivité et facilité d'utilisation, et devront être tenues à jour. Des données de mauvaise qualité impliquent des risques. La qualité des données doit être évaluée afin de déterminer l'existence de données biaisées susceptibles d'entraîner une discrimination illégale et arbitraire. Le traitement automatique des données devra être évité, en particulier lorsqu'il est susceptible d'avoir un impact sur des individus ou groupes d'individus. En outre, une évaluation périodique de la qualité des données est recommandée pendant le cycle de vie de ces dernières.

8. DONNÉES OUVERTES, TRANSPARENCE ET RESPONSABILITÉ

Les données ouvertes constituent un moteur important d'innovation, de transparence et de responsabilité. Dans la mesure du possible, les données devront être ouvertes, à moins que les risques liés au fait de les rendre ouvertes ne l'emportent sur les avantages, ou qu'il y ait d'autres raisons légitimes de ne pas le faire. Il est également important de mettre en place des mécanismes appropriés de gouvernance et de responsabilisation afin de garantir le respect des dispositions légales pertinentes. La transparence est un élément essentiel en matière de responsabilité. La nature, la durée de conservation prévue et la finalité de l'utilisation des données, ainsi que les algorithmes utilisés pour les traiter devront être rendus publics et décrits dans un langage clair et non technique, adapté au grand public.

9. VÉRIFICATIONS PRÉALABLES CONCERNANT LES COLLABORATEURS TIERS

Les collaborateurs tiers qui participent à l'utilisation des données devront agir dans le respect des lois applicables, notamment celles relatives à la protection de la vie privée, et respecter les normes les plus strictes en matière de confidentialité et de conduite morale et éthique. Afin de garantir la conformité, il est recommandé qu'un processus de vérification préalable soit mené afin d'évaluer les pratiques en matière de données des éventuels collaborateurs tiers. De plus, des accords juridiquement contraignants décrivant les paramètres d'accès aux données et de traitement des données devront être conclus.

African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
www.au.int