AfriSIG 2024 : Consultation multipartite sur la mise en œuvre du protocole numérique de la Zone de libre-échange continentale africaine (ZLECAf) conformément au Cadre politique de l'Union Africaine en matière de données

Résultat de l'Exercice Pratique

Préambule

1. Ce document décrit les opportunités et les défis liés à l'harmonisation du Protocole sur le Commerce Numérique (le Protocole) dans le cadre de la Zone de libre-échange continentale africaine (ZLECAf), adopté en février 2024 et du Cadre de politique de l'Union Africaine en matière de données (ci-après dénommé l'AUDPF), adopté en juillet 2022. Son objectif est d'identifier les défis, de proposer des solutions concrètes et de contribuer à la mise en œuvre effective de deux annexes essentielles du Protocole, soutenant la vision de l'Afrique pour une économie numérique unifiée, inclusive et durable, à savoir (i) les transferts de données transfrontaliers et (ii) les critères permettant de déterminer les raisons publiques légitimes de divulgation du code source. Nous pensons que ce document sera utile au Secrétariat de la ZLECAf, aux États membres et à d'autres organisations régionales, y compris les Communautés Économiques Régionales (CER).
2. Les réflexions et recommandations incluses dans ce document sont le résultat d'un effort de collaboration entre des individus de divers groupes de parties prenantes, y compris les gouvernements, les membres du Parlement, les entreprises, la société civile, les organisations intergouvernementales, les médias, les institutions de recherche et la communauté technique qui ont participé à la 11ème édition de l'École Africaine sur la Gouvernance de l'Internet

(AfriSIG) qui s'est tenue à la Commission Économique des Nations Unies pour l'Afrique à Addis-Abeba, Éthiopie, du 14 au 19 novembre 2024.

3. Ses auteurs reconnaissent le potentiel transformateur de la ZLECAf pour accélérer le commerce intra-africain et renforcer la position commerciale de l'Afrique sur le marché mondial. Ils reconnaissent également l'importance d'aligner le Protocole sur l'AUDPF afin d'éviter les défis liés aux désalignements politiques et de contribuer au développement de l'infrastructure numérique dans la région. Nous pensons que surmonter ces défis renforcera l'intégration régionale, accélérera la croissance économique et favorisera un développement équitable dans tous les États membres, en particulier pour les communautés marginalisées.

Section A : Remarques générales sur le Protocole Numérique de la ZLECAf et l'AUDPF

L'adoption en février 2024 du Protocole Numérique de la ZLECAf par le 37e Sommet des Chefs d'État de l'Union africaine (UA) a abouti à la création du premier cadre régional sur le commerce numérique en Afrique, qui couvre 54 pays et couvre la plus grande zone de libre-échange au monde.

Le Protocole envisage une industrialisation numérique en Afrique en créant un environnement propice au commerce et à l'innovation numériques. Il établit des règles et des principes harmonisés en matière de commerce numérique qui peuvent réduire les coûts des transactions commerciales, améliorer l'accès aux marchés régionaux et stimuler l'entrepreneuriat numérique. Il représente un potentiel important pour l'Afrique dans la mise en place d'un marché numérique unique unifié et interopérable et est conforme à l'Agenda 2063 et à la Stratégie de transformation numérique 2020-2030 de l'UA.

L'AUDPF, élaborée en 2022, offre des avantages significatifs pour la gouvernance des données en Afrique. Il fournit des conseils pour naviguer dans des questions réglementaires complexes, soutient le commerce numérique intra-africain, l'entrepreneuriat et l'innovation, et établit des garde-fous contre les risques et les préjudices potentiels découlant de l'économie numérique. En particulier, il soutient le transfert transfrontalier de données, en favorisant l'innovation et l'expansion sur de nouveaux marchés ; nécessite une montée en compétences, en créant des opportunités pour les professionnels de l'économie numérique ; assure une concurrence loyale en empêchant les comportements monopolistiques dans l'économie numérique ; promeut la création de pôles d'innovation pour favoriser la collaboration entre les entrepreneurs, les chercheurs et les décideurs technologiques ; fait progresser la recherche et le développement dans les technologies émergentes et protège la propriété intellectuelle tout en permettant la divulgation du code source pour des raisons impérieuses d'intérêt public.

L'AUDPF présente une feuille de route pour la gestion des données à travers l'Afrique, en mettant l'accent sur un écosystème fiable, sécurisé et inclusif qui équilibre les

avantages de l'innovation en matière de données avec le besoin de confidentialité, de sécurité et de gouvernance éthique. Il vise à harmoniser les politiques entre les États membres, en favorisant la collaboration et l'interopérabilité, essentielles à la réalisation des objectifs du protocole et à l'établissement d'un marché unique numérique dans la région.

Une gouvernance efficace des données est essentielle au succès du Protocole et à la garantie de politiques économiques équitables. L'alignement des politiques nationales en matière de données sur ce cadre peut soutenir la coopération régionale et les objectifs de la ZLECAf, en intégrant les données personnelles et non personnelles pour éclairer les stratégies économiques et promouvoir l'inclusion. L'alignement des annexes du Protocole sur l'AUDPF constituerait une étape clé vers la prise en compte de la diversité réglementaire de l'Afrique en permettant une approche cohérente des transferts transfrontaliers de données, tout en répondant aux préoccupations liées aux droits de propriété intellectuelle, à la protection des données et à la cybersécurité.

Des lois complètes sur la protection des données, des autorités indépendantes de protection des données et l'autonomisation de la société civile sont essentielles pour assurer la protection des droits numériques, tout comme l'élaboration de cadres co-juridictionnels permettant une gouvernance efficace de l'économie numérique. L'AUDPF reconnaît qu'il est complexe d'harmoniser les politiques de données existantes pour renforcer la confiance dans l'écosystème. Il permet néanmoins aux États de préserver leurs intérêts souverains tout en concevant et en révisant des politiques qui servent les intérêts du continent. De cette façon, il sert de ressource de référence clé pour les États membres lorsqu'ils conçoivent et examinent leurs politiques et instruments juridiques de gouvernance des données, contribuant ainsi à un paysage unifié, sécurisé et avant-gardiste de la gouvernance des données.

La mise en œuvre de l'AUDPF nécessite une collaboration entre les États membres de l'UA, les parties prenantes du secteur privé, la communauté technique et les organisations de la société civile, en veillant à ce que leurs intérêts et préoccupations respectifs soient pris en compte de manière adéquate. L'AUDPF souligne également l'importance de la souveraineté et de la propriété des données. Il encourage les pays à mettre en place des systèmes de données nationaux qui renforcent les institutions locales et maintiennent l'indépendance numérique du continent. L'équilibre entre les flux de données transfrontaliers et la souveraineté des données nécessite également le respect de la confidentialité et de la sécurité afin d'éviter les abus et les violations.

Les transferts transfrontaliers de données destinés à faciliter la libre circulation des données entre les pays africains pour soutenir le commerce numérique ne doivent pas privilégier les intérêts des entreprises au détriment de la souveraineté des données et de la protection des informations personnelles. Des flux de données illimités pourraient permettre à des entreprises privées d'exploiter les marchés africains des données sans garanties adéquates, ce qui pourrait conduire à l'exploitation des données et à la perte de contrôle des informations personnelles sensibles.

Bien que le Cadre soit un atout stratégique permettant le développement, des défis subsistent, tels que les disparités dans la mise en œuvre entre les États membres, les

différents niveaux de préparation numérique et la nécessité de mobiliser la volonté politique nécessaire. Il existe également d'importantes disparités en matière d'infrastructure numérique et de participation à l'économie numérique entre les pays africains. L'AUDPF est un outil d'orientation important qui harmonise les cadres de gouvernance des données existants et établit des intersections entre les droits des données et la vie privée sans compromettre l'accès facile aux données et aux informations.

La mise en œuvre du Protocole doit donner la priorité aux initiatives qui comblent ce fossé en améliorant l'accès à Internet et la culture numérique. Une approche qui tient compte des déséquilibres structurels en matière de pouvoir et d'accès aux ressources et qui donne la priorité à l'inclusion des groupes exclus peut également contribuer à réduire la fracture numérique et à promouvoir des opportunités commerciales équitables, en particulier pour les initiatives et les entreprises dirigées par des femmes et situées dans les communautés rurales. Dans ce contexte, les petites et moyennes entreprises (PME) doivent être fortement mises en avant et les défis auxquels elles sont confrontées doivent être pris en considération, afin de s'assurer qu'elles bénéficient du libre-échange numérique en Afrique.

Le Protocole devrait déclencher une vague d'industrialisation et de diversification en réduisant les obstacles au commerce et en s'attaquant aux principaux catalyseurs du commerce numérique, tels que les transferts de données transfrontaliers, la réglementation du commerce électronique et la fiscalité numérique. À cet égard, il est également nécessaire d'accélérer la mise en œuvre du Système Panafricain de Paiement (PAPPS). L'AUDPF, le Protocole et d'autres initiatives de gouvernance des données constituent collectivement des éléments importants de l'intégration régionale de l'Afrique et de la poursuite de la transformation numérique, en particulier dans les domaines de l'élaboration des politiques, de l'innovation et de la croissance économique.

Section B : Défis et préoccupations

Nous reconnaissons que l'harmonisation du Protocole avec l'AUDPF se heurte à des défis critiques. L'un des principaux éléments est la disparité des politiques et des réglementations entre les États membres, en particulier en ce qui concerne la protection des données, la confidentialité, la cybersécurité et la fiscalité numérique. Des législations nationales divergentes créent des incohérences qui entravent le développement d'un environnement commercial numérique unifié. Les politiques relatives à la circulation transfrontalière des données compliquent encore l'harmonisation, de nombreux pays imposant des restrictions motivées par des préoccupations concernant la souveraineté et la sécurité des données.

Alors que le Protocole promeut l'élimination des obstacles à la circulation des données, le fait qu'il autorise des restrictions fondées sur des préoccupations légitimes introduit des ambiguïtés qui pourraient entraver l'intégration régionale et l'accès préférentiel aux données pour les Africains, comme envisagé par l'AUDPF. Cela crée une couche

supplémentaire de complexité réglementaire, ce qui peut alourdir le fardeau des gouvernements et retarder la mise en œuvre.

De nombreux pays ont des lois disparates en matière de protection des données, ce qui complique la conformité pour les entreprises opérant au-delà des frontières. Cette incohérence peut entraîner des incertitudes juridiques et une augmentation des coûts opérationnels pour les entreprises qui tentent de naviguer dans plusieurs environnements réglementaires.

La disposition du Protocole selon laquelle les pays africains ne devraient pas exiger la divulgation du code source s'aligne sur la promotion de l'innovation et l'attraction des investissements étrangers. Cependant, nous croyons que cette position doit faire l'objet d'un examen nuancé afin d'établir un équilibre entre les intérêts économiques et les préoccupations stratégiques et de sécurité. Bien que l'interdiction générale de la divulgation du code source protège les technologies propriétaires, elle peut limiter la capacité des gouvernements à s'assurer que les produits numériques respectent les normes de sécurité et d'éthique. Ceci est particulièrement critique dans des secteurs tels que la santé, la finance et la sécurité nationale, où les vulnérabilités des logiciels peuvent avoir de graves conséquences.

Le manque de clarté entourant la non-divulgation des codes source pose également des défis importants. La position actuelle du Protocole qui décourage la divulgation obligatoire soulève des préoccupations quant à la responsabilité et à l'équité, en particulier lorsqu'il s'agit de négocier avec de grands fournisseurs de technologie étrangers. En outre, les disparités en matière d'infrastructures numériques et de connectivité à travers le continent exacerbent les inégalités dans l'adoption de politiques harmonisées. L'engagement limité des parties prenantes, en particulier avec le secteur privé, la société civile et les groupes marginalisés, compromet l'inclusion, tandis qu'un accent insuffisant sur l'égalité des sexes et les droits numériques risque de perpétuer les inégalités. La dépendance excessive à l'égard des fournisseurs de technologies étrangers, tels que les services cloud, met encore plus à mal la souveraineté numérique de l'Afrique.

Les transferts transfrontaliers de données et la divulgation des codes source doivent avoir lieu en tenant compte des éléments suivants :

a. Protéger la confidentialité et la sécurité des données et souligner la nécessité de mesures de protection pour garantir que les données personnelles sont traitées de manière responsable au-delà des frontières.
b. Prévenir l'exploitation des données en veillant à ce que l'extraction de données provenant de pays en développement sans avantages économiques adéquats ni garanties de souveraineté soit empêchée.
c. L'impact des inégalités potentielles dans le commerce numérique qui favorisent les entreprises technologiques multinationales par rapport aux startups locales, aux petites entreprises et aux groupes marginalisés pour garantir l'inclusion et l'équité.
d. Des critères clairs pour déterminer les raisons publiques légitimes de la divulgation du code source.

e. Veiller à ce que les gouvernements aient le droit d'exiger la divulgation du code source dans les cas où la sécurité publique, les droits numériques ou la surveillance réglementaire sont en jeu.

f. Reconnaître l'importance de protéger la propriété intellectuelle, mais rejeter les protections générales qui pourraient masquer les pratiques préjudiciables ou réduire la confiance des consommateurs en équilibrant l'innovation et la surveillance.

g. Éduquer les citoyens par le biais de campagnes de sensibilisation à leurs droits numériques, tout en plaidant pour des politiques inclusives et des accords de partage de données équitables, peut lutter contre les inégalités et soutenir la transformation numérique de l'Afrique en s'engageant stratégiquement dans ces cadres.

La collaboration multipartite est cruciale et peut donner lieu à des recommandations concrètes sur l'inclusion numérique, l'innovation et l'utilisation éthique des technologies émergentes. Les parties prenantes doivent également promouvoir l'inclusion numérique en promouvant un accès équitable aux TIC, à un internet abordable et au développement des compétences numériques, en particulier pour les groupes marginalisés tels que les femmes, les populations rurales et les personnes handicapées.

De nombreux pays africains ne disposent pas des ressources et des capacités institutionnelles nécessaires pour mettre en œuvre efficacement des lois complètes sur la protection des données. Cet écart peut conduire à une application inégale de la réglementation, créant un désavantage concurrentiel pour les entreprises dans les régions où les cadres réglementaires sont plus faibles. Par exemple, un obstacle important à l'harmonisation de la gouvernance des données est le manque de clarté concernant la protection des données et les responsabilités en matière de propriété. Cette ambiguïté peut empêcher les entreprises d'investir en toute confiance dans des innovations axées sur les données, car elles peuvent ne pas être certaines de leurs droits et responsabilités sur les données qu'elles collectent et traitent. De plus, cela crée une hésitation chez les entreprises à l'égard de l'innovation axée sur les données et du transfert ou du partage de données au-delà des frontières, car elles peuvent craindre d'enfreindre les droits ou les réglementations d'une autre juridiction.

En l'absence de lois, de réglementations et de pratiques strictes en matière de sécurité numérique dans chaque pays, l'harmonisation de la protection des données et des protocoles numériques à travers le continent exposera les entreprises à une cybercriminalité croissante, non seulement sur le continent, mais aussi dans d'autres régions. Si l'on ne s'attaque pas à ces obstacles, les efforts visant à harmoniser le Protocole de commerce numérique de la ZLECAf avec l'AUDPF risquent de se fragmenter, ce qui réduira le potentiel du commerce numérique à favoriser une intégration régionale transformatrice en Afrique.

L'AUDPF fournit des orientations générales sur les transferts transfrontaliers de données, mais manque de précision pour opérationnaliser ces principes dans le cadre de la ZLECAf. La mise en œuvre est ambiguë et, en l'absence de normes claires, les

processus techniques permettant d'assurer la protection des données lors des transferts transfrontaliers sont laissés à l'abandon, ce qui augmente les risques de non-conformité. Les pays qui appliquent des règles plus strictes en matière de transferts transfrontaliers peuvent créer des obstacles au commerce, ce qui compromet les objectifs du Protocole.

Trouver un équilibre entre l'innovation et la réglementation : en conciliant la protection de la vie privée et la promotion de l'innovation et du commerce numériques. « Les données à caractère personnel collectées sur le territoire d'un État partie ne peuvent être transférées vers un autre État partie qu'avec l'autorisation préalable de l'autorité de protection des données ». Des règles de protection des données ouvertement strictes peuvent freiner l'innovation, en particulier pour les start-ups et les PME qui n'ont pas les ressources nécessaires pour s'y conformer, mais des réglementations faibles ou incohérentes peuvent également exposer les entreprises et les particuliers à des vulnérabilités en matière de confidentialité et de sécurité des données.

Les critères de divulgation du code source doivent garantir la transparence, car cela est essentiel pour favoriser la confiance et l'innovation. Cependant, il est important de trouver un équilibre entre l'intérêt public et les risques d'entraver l'innovation et d'exposer les entreprises à une concurrence déloyale.

L'annexe au Protocole concernant la divulgation du code source met l'accent sur la protection de la propriété intellectuelle tout en prévoyant des exceptions dans des conditions spécifiques d'intérêt public afin de garantir que les entreprises ne soient pas obligées de divulguer le code d'un logiciel propriétaire comme condition préalable à l'accès au marché. Cependant, des protections aussi larges peuvent limiter la surveillance, en particulier dans des domaines tels que la cybersécurité, la transparence des algorithmes et les droits numériques.

L'annexe ne définit pas clairement les « raisons légitimes d'intérêt public » qui permettraient aux gouvernements d'exiger la divulgation du code source, en particulier dans les scénarios impliquant la santé, la sécurité et le bien-être publics. Bien que ce manque de clarté diverge actuellement des pratiques observées dans des régions comme l'Europe, qui applique des réglementations numériques plus strictes en matière de transparence, il est possible de s'aligner à l'avenir sur les meilleures pratiques. Cet alignement serait essentiel pour les États africains alors que nous cherchons à équilibrer efficacement le commerce numérique avec la protection des données, y compris les données personnelles des personnes participant au commerce numérique.

Dans le même temps, les règles sur les flux de données transfrontaliers et l'accès au code source, qui visent à faciliter la libre circulation des données et le commerce numérique au sein du continent, ne devraient pas renforcer par inadvertance la domination des entreprises technologiques étrangères (non africaines) en Afrique, ce qui pourrait entraver le transfert de technologie crucial pour le développement de l'économie numérique émergente de l'Afrique.

Les États doivent fournir des garanties par le biais de leur législation et de leurs politiques nationales pour les industries africaines, en particulier les petites et moyennes entreprises. Ils devraient également adopter des mesures visant à encourager le transfert de technologie, telles que l'imposition ou l'incitation à la conclusion d'accords de transfert dans le cadre des conditions d'accès au marché pour les entreprises liées à des pays non africains lorsque cela est justifié, et renforcer les lois sur la concurrence pour empêcher les tendances ou les pratiques monopolistiques des entreprises étrangères (y compris les géants de la technologie) qui étouffent l'innovation africaine.

Section C: Propositions et recommandations

Les propositions et recommandations suivantes visent à aider le Secrétariat de la ZLECAf, les États membres, les autres organismes de mise en œuvre, les entreprises individuelles et toutes les autres parties prenantes, à mettre en œuvre efficacement et à développer le Protocole d'une manière harmonisée avec l'AUDPF.

Recommandations générales

Nous vous recommandons de, d’:

1. Investir dans des initiatives de renforcement des capacités. Mettre en place des mécanismes régionaux pour fournir une assistance technique et une formation spécialisée aux régulateurs et aux parties prenantes, y compris les entités commerciales. Cela aiderait les États membres à mettre en œuvre des politiques efficaces de gouvernance des données et à développer l'infrastructure nécessaire à la mise en œuvre du Protocole. La mise en place et le renforcement de mécanismes régionaux de renforcement des capacités sont essentiels. Ceux-ci fourniraient une assistance technique aux États membres pour la mise en œuvre du Protocole et le développement de l'infrastructure nécessaire à la gouvernance des données.
2. Renforcer le mécanisme de mise en œuvre du Protocole : Le mécanisme de mise en œuvre du Protocole sur le commerce numérique de la ZLECAf, tel qu'il est actuellement dévolu à un comité du Secrétariat de la ZLECAf, semble présenter certaines faiblesses. Nous proposons la création d'un organe de mise en œuvre spécifique au sein du Secrétariat, doté d'un mandat spécifique pour superviser l'exécution du Protocole. Cet organisme devrait avoir le pouvoir de surveiller la conformité, de fournir un soutien technique et de traiter les litiges.
3. Élaborer une législation nationale complète sur la gouvernance des données : Les pays sont invités à établir des lois nationales sur la protection des données personnelles qui s'alignent sur les principes énoncés dans la Convention de Malabo de l'UA. Cette législation devrait donner la priorité à des structures de gouvernance des données bien définies qui renforcent la confiance dans les environnements numériques. Assurer un équilibre entre la facilitation des échanges et la souveraineté des données : Élaborer des politiques qui alignent

les efforts de facilitation du commerce international sur la nécessité de protéger la souveraineté nationale des données.

4. Veiller à ce que les lois nationales sur la protection des données contiennent explicitement des dispositions visant à empêcher l'exploitation des données. Ces lois devraient inclure des garanties pour garantir que les données extraites des pays africains produisent des avantages économiques significatifs et la protection de la souveraineté.
5. La promotion de l'interopérabilité et des normes de données ouvertes : Nous recommandons de développer des mécanismes d'interopérabilité et d'établir des normes de données ouvertes. Cela faciliterait l'échange de données non personnelles, y compris l'échange entre chercheurs et entrepreneurs, tout en assurant le respect des principes de protection de la vie privée.
6. Lancer des campagnes de sensibilisation. Développer des initiatives pour éduquer les citoyens sur leurs droits numériques.
7. Investir dans un environnement propice à l'essor du commerce numérique. Il s'agit notamment d'assurer un accès équitable aux TIC, à un internet abordable et à la formation aux compétences numériques, en particulier pour les groupes marginalisés.
8. Assurer l'inclusion et l'équité : Identifier et mettre en évidence l'impact des inégalités potentielles dans le commerce numérique qui favorisent les entreprises technologiques multinationales par rapport aux entreprises locales en démarrage, aux petites entreprises et aux groupes marginalisés. Pour remédier à ces inégalités, il convient d'encourager l'innovation locale, de promouvoir une concurrence loyale et d'apporter un soutien réglementaire aux entreprises locales afin de faciliter un accès équitable aux opportunités de commerce numérique.

Recommandations sur les flux de données transfrontaliers

9. Nous reconnaissons l'importance de supprimer les obstacles aux flux de données transfrontaliers afin de faciliter le commerce numérique et l'intégration économique dans le cadre de la ZLECAf. Cependant, la disposition actuelle du protocole permettant aux pays de restreindre ces flux sur la base de « préoccupations légitimes » introduit une ambiguïté et des défis réglementaires potentiels. Cette condition impose un fardeau réglementaire supplémentaire à plusieurs parties prenantes, y compris les parlements, car ils sont chargés de définir et de superviser ce qui constitue des « préoccupations légitimes ». L'absence de critères clairs crée un risque d'interprétations incohérentes entre les États membres, ce qui pourrait compromettre les objectifs d'harmonisation du protocole. De plus, le manque de clarté peut décourager l'investissement et l'innovation en créant de l'incertitude pour les entreprises qui exercent leurs activités au-delà des frontières. Pour remédier à cette situation, nous proposons les ajouts suivants à l'annexe sur les flux de données transfrontaliers :

9.1 Définir les « préoccupations légitimes » : Fournir une définition claire et étroite des préoccupations légitimes, y compris des motifs spécifiques tels que la sécurité nationale, la santé publique et la protection des droits fondamentaux.

9.2 Établir des mécanismes de surveillance, de conformité et de soutien à la mise en œuvre. Cela pourrait impliquer la mise en place d'un organe de surveillance sous l'égide du Secrétariat de la ZLECAf pour examiner, conseiller et, le cas échéant, approuver toute restriction sur les flux de données transfrontaliers afin d'assurer le respect du Protocole.

9.3 Transparence du mandat : Exiger des États membres qu'ils divulguent publiquement les raisons et les preuves de l'imposition de restrictions, en veillant à ce que la responsabilité soit rendue.

9.4 Encourager la proportionnalité : Préciser que toute restriction doit être le moyen le moins restrictif de répondre à des préoccupations légitimes, conformément aux normes internationales.

Nous vous recommandons également:

10. La facilitation d'accords de reconnaissance mutuelle entre les États membres afin de reconnaître les cadres de protection des données de l'autre, permettant ainsi des flux de données fiables et transparents.
11. L'intégration des marchés et la normalisation des systèmes de paiement et de taxation en ligne visant à faciliter les flux de données et le commerce transfrontaliers tout en veillant à ce qu'aucun droit de douane ne soit imposé sur les produits numériques conformément au Protocole.

Recommandations sur la divulgation du code source

L'accès au code source doit être autorisé pour des raisons de sécurité nationale, de sécurité publique et de conformité réglementaire. Un contrôle par des organes judiciaires ou indépendants est nécessaire pour se protéger contre les actions arbitraires, et des accords de confidentialité devraient être obligatoires pour protéger la propriété intellectuelle. Des processus clairs et transparents de demande de code source doivent être établis afin d'éviter toute utilisation abusive.

Nous vous recommandons:

12. L'introduction de la divulgation conditionnelle : Permettre aux gouvernements d'exiger la divulgation du code source à des fins spécifiques et étroitement définies, telles que les audits de cybersécurité ou la sécurité publique, dans le cadre d'accords de confidentialité stricts.
13. L’utilisation les mécanismes de résolution des litiges prévus par le Protocole pour résoudre les conflits découlant des demandes de divulgation du code source, en garantissant l'équité et la cohérence de la prise de décision.

14. L’établissement des lignes directrices sur le moment et la manière dont le code source peut être examiné afin d'assurer la cohérence entre les États membres et d'éviter les abus.
15. La promotion de l'utilisation de normes ouvertes et de solutions libres pour les marchés publics afin d'accroître la transparence, de réduire la dépendance à l'égard des technologies exclusives et de favoriser l'innovation.
16. L’amélioration de la transparence et la responsabilisation en encourageant les gouvernements à adopter des cadres qui leur permettent de demander la divulgation des codes sources lorsque cela est nécessaire pour protéger la sécurité publique, les droits numériques ou assurer la conformité réglementaire.
17. Trouver un équilibre entre l'innovation et la surveillance : Protéger les droits de propriété intellectuelle tout en s'opposant aux protections générales qui pourraient favoriser des pratiques néfastes ou éroder la confiance des consommateurs.

Ces approches équilibrées en matière de flux de données transfrontaliers et de divulgation du code source garantissent que le Protocole s'aligne sur les objectifs de l'AUDPF tout en préservant les intérêts africains et en répondant aux préoccupations légitimes. En tant que parlementaires, gouvernements, société civile, membres du monde des affaires, de la communauté technique et des médias, ainsi que des chercheurs et des organisations internationales, nous nous engageons à affiner ces dispositions pour contribuer à un cadre de gouvernance des données transfrontalières solide et exécutoire qui soutient la transformation numérique de l'Afrique.

Conclusions

Cette collaboration marque un moment décisif dans la vision de l'Afrique d'établir un marché numérique unifié, inclusif et durable qui renforce l'intégration régionale, la croissance économique avancée et soutient le développement équitable entre les États membres. Tout en reconnaissant l'immense potentiel du protocole et de l'AUDPF, nous comprenons également la complexité de l'harmonisation des politiques dans divers contextes juridiques et réglementaires. Il reste essentiel de relever les défis, tels que les disparités dans les cadres nationaux de protection des données, d'équilibrer la souveraineté des données et la libre circulation de l'information, et d'assurer la protection des droits numériques. Nous devons continuer à relever ces défis avec prudence, en veillant à ce que le commerce numérique soit non seulement facilité, mais aussi d'une manière qui respecte la souveraineté des États membres de l'UA et préserve les intérêts de toutes les parties prenantes.

Les propositions et les recommandations contenues dans ce document proposent des mesures concrètes pour surmonter ces défis, en mettant l'accent sur la création d'un cadre clair et cohérent pour les transferts de données transfrontaliers et la divulgation du code source.

À mesure que nous avançons, nous devons maintenir une approche collaborative multipartite qui inclut les entreprises gouvernementales, la société civile et les experts techniques. Ce n'est qu'à travers des efforts concertés et un dialogue continu que nous pourrons faire en sorte que la ZLECAf et l'AUDPF réalisent leur potentiel de transformation. Nous restons déterminés à travailler avec toutes les parties pour affiner et mettre en œuvre les cadres nécessaires qui favoriseront la transformation numérique et montreront que les avantages du commerce numérique sont répartis, équitablement et durablement, sur l'ensemble du continent.