ANNEXES COMPILÉES
AU
PROTOCOLE SUR LE COMMERCE NUMÉRIQUE
DE LA ZONE DE LIBRE-ÉCHANGE CONTINENTALE AFRICAINE

ANNEXE
SUR LES RÈGLES D'ORIGINE

PREMIÈRE PARTIE
DISPOSITIONS GÉNÉRALES

Article premier
Définitions

Aux fins de la présente Annexe, l'on entend par :

a. **« Annexe »**, l'annexe sur les Règles d'origine du protocole ;

b. **« Contenu »**, un produit numérique tel que défini à l'article 1(h) du Protocole ;

c. **« Plateforme numérique »,** une interface numérique ou une application qui permet des interactions et des transactions entre entreprises et/ou consommateurs pour faciliter le commerce numérique, y compris, mais sans s'y limiter, les marchés en ligne, les plateformes d'économie collaborative ou de partage, les plateformes de communication, les réseaux sociaux en ligne, les moteurs de recherche en ligne, les navigateurs web, les cartes en ligne, les agrégateurs d'actualités, les plateformes musicales, les plateformes de partage de vidéos et d'autres médias, les systèmes de paiement numérique, les magasins d'applications, les plateformes de publicité en ligne, les systèmes d'exploitation et les services d'intermédiation en ligne ;

d. **« Entreprise »,** toute personne morale dûment constituée, enregistrée ou autrement incorporée et exploitée en vertu des lois et règlements applicables d'un État partie ;

e. **« Personne morale »**, une entité juridique dûment constituée, enregistrée ou autrement incorporée et exploitée en vertu des lois et règlements applicables d'un État partie ;

f. « **Personne physique »**, un ressortissant d'un État partie conformément à ses lois et règlements. Il est entendu qu'une personne physique qui possède une double nationalité est réputée être exclusivement un ressortissant du pays dont elle a la nationalité effective ou dans lequel elle réside habituellement ou en permanence ;

g. **« Personne d'un État partie »,** une personne d'un État partie telle que définie à l'article 1(p) du Protocole ; et

h. **« Règles d'origine »,** les règles établies dans la présente Annexe pour déterminer l'origine des entreprises à capitaux africains, des plateformes numériques africaines et du contenu africain, ainsi que des produits numériques, conformément à l'article 5 du Protocole.

Article 2
Objectifs

Les objectifs de de la présente Annexe sont :

a. donner effet à l'article 5 du Protocole ;

b. faciliter le développement du marché numérique de la ZLECAf ;

c. promouvoir le développement et la croissance des entreprises africaines, des plateformes numériques africaines et des contenus ;

d. promouvoir le commerce de contenus par des entreprises à capitaux africains et l'utilisation de plateformes numériques africaines ; et

e. établir des critères transparents et prévisibles pour déterminer l'éligibilité au traitement préférentiel en vertu du Protocole.

DEUXIÈME PARTIE

CHAMP D'APPLICATION DES PRODUITS NUMÉRIQUES

Article 3

Produits numériques

1. Conformément à l'article 1(h) du Protocole, les produits numériques couverts par le Protocole comprennent :

a. les programmes électroniques ;
b. les textes ;
c. les vidéos ;
d. les images ;
e. les enregistrements sonores ; ou
f. tout autre produit codé numériquement, produit pour la vente ou la distribution commerciale et pouvant être transmis électroniquement.

2. La représentation numérisée d'un instrument financier, y compris de l'argent, n'est pas couverte en tant que produit numérique par le Protocole.

TROISIÈME PARTIE

ORIGINE D'UNE ENTREPRISE À CAPITAUX AFRICAINS, D'UNE PLATEFORME NUMÉRIQUE AFRICAINE ET D'UN CONTENU AFRICAIN

Article 4

Entreprise à capitaux africains

1. Une entreprise à capitaux africains est une entité juridique dûment constituée, enregistrée ou autrement incorporée et exploitée en vertu des lois et règlements applicables d'un État partie, détenue et contrôlée par une personne physique ou morale d'un État partie ou d'États parties, et qui exerce des activités commerciales importantes sur le territoire d'un État partie.

2. Il est entendu qu'une entreprise à capitaux africains est :

a. détenue par une ou des personne(s) physique(s) ou morale(s) d'un État partie ou d'États parties si cette personne détient plus de 50% des parts de l'entreprise ; et

b. contrôlée par une ou plusieurs personnes physiques ou morales d'un ou de plusieurs État parties, si cette personne a le pouvoir de nommer la majorité des administrateurs ou de diriger légalement les opérations de l'entreprise.

3. Les opérations commerciales substantielles visées au présent article sont évaluées conformément à l'expression « activité substantielle » définie à 'article premier du Protocole sur les investissements.

4. Conformément à l'alinéa 3 de l'article 22 du Protocole, les États parties encouragent les entreprises africaines à créer et à utiliser des installations informatiques sur leur territoire.

Article 5

Plateforme numérique africaine

1. Une plateforme numérique comme définie à l'article 1(c) de la présente Annexe est africaine si elle dûment constituée, enregistrée ou autrement incorporée et exploitée en vertu des lois et règlements applicables d'un État partie et si elle est détenue et contrôlée par une ou plusieurs personnes physiques ou morales d'un État partie ou d'États parties.

2. Il est entendu qu'une plateforme numérique africaine est :

a. détenue par une ou plusieurs personnes physiques ou morales d'un ou de plusieurs États parties si cette ou ces personnes détiennent plus de 50 % des parts de la plateforme numérique ; et
b. contrôlée par une ou plusieurs personnes physiques ou morales d'un ou de plusieurs États parties, si cette ou ces personnes ont le pouvoir de nommer une majorité de ses administrateurs ou de diriger légalement les opérations de la plateforme numérique.

3. Conformément à l'alinéa 3 de l'article 22 du Protocole, les États parties encouragent les plateformes numériques africaines à utiliser des installations informatiques établies dans les États parties.

4. Les États parties favorisent et encouragent la création et l'utilisation de plateformes numériques africaines par les entreprises à capitaux africains.

Article 6

Contenu africain

1. Le contenu est africain s'il est la propriété d'une personne physique ou morale d'un État partie, conformément aux lois et règlements applicables d'un État partie.

2. Il est entendu que le contenu africain doit être interprété comme un produit numérique originaire des États parties, comme le stipule l'alinéa 1 de l'article 6 du Protocole.

Article 7

Éligibilité au traitement préférentiel

1. Le contenu africain échangé par des entreprises à capitaux africains ou des ressortissants d'États parties, ou diffusé sur des plateformes numériques africaines, peut bénéficier d'un traitement préférentiel au titre du Protocole.

2. Dans l'application de la présente Annexe, les États parties accordent un traitement favorable aux jeunes entreprises (start-ups), aux micro, petites et moyennes entreprises (PME), aux femmes, aux jeunes, aux peuples autochtones, aux communautés rurales et locales, aux personnes handicapées et aux autres groupes sous-représentés africains.

QUATRIÈME PARTIE

PROMOTION DU COMMERCE NUMÉRIQUE INTRA-AFRICAIN

Article 8

Mesures visant à promouvoir le commerce numérique intra-africain

Les États parties sont encouragés à introduire des mesures visant à promouvoir le développement d'entreprises détenues par des Africains, de plateformes numériques africaines et de contenus africains. Les mesures visées dans le présent article consistent notamment, sans s'y limiter, à ce qui suit :

a. fournir un appui technique et financier visant à développer le contenu africain, les entreprises détenues par des Africains et les plateformes numériques africaines ;
b. promouvoir et faciliter l'utilisation du domaine « point Africa » (.africa) par les entreprises africaines, les plateformes numériques africaines et les ressortissants des États parties ;
c. créer un fonds dans le cadre du Fonds d'ajustement de la ZLECAf qui accepte les contributions volontaires des États parties, du secteur privé, des partenaires de développement et d'autres parties prenantes pour le développement et la croissance du contenu africain, des entreprises détenues par des Africains et des plateformes numériques africaines ;
d. promouvoir le développement et l'amélioration des plateformes numériques afin de favoriser une plus grande participation des MPME, des femmes, des jeunes, des peuples autochtones, des communautés rurales et locales, des personnes vivant avec un handicap, et d'autres groupes sous-représentés dans le commerce numérique grâce, entre autres, à des financements par le biais de remises sur les frais d'intégration, d'abonnement et de crédits publicitaires ou de promotions ciblées ;
e. favoriser le transfert de technologies, de compétences, de savoir-faire, d'innovations et d'autres avantages entre des entreprises ou des plateformes numériques étrangères et africaines afin de renforcer les capacités africaines ;
f. encourager les entreprises, les plateformes et les créateurs de contenu internationaux à contribuer au développement des entreprises, des plateformes numériques et des créateurs de contenus africains par le biais d'une aide financière et du développement des compétences ;
g. réduire les disparités économiques et de développement des MPME, des femmes, des jeunes, des populations autochtones, des personnes handicapées, des communautés rurales et locales, et d'autres groupes sous-représentés ; et
h. fournir une formation dans la recherche, l'ingénierie, la conception et d'autres domaines pertinents relatifs au développement de plateformes numériques africaines, de contenus africains et de produits numériques.

CINQUIÈME PARTIE

DISPOSITIONS FINALES

Article 9

Règlements et lignes directrices

Les États parties peuvent développer des réglementations ou des lignes directrices continentales sur l'un des aspects de la présente Annexe afin de faciliter sa mise en œuvre et son application effectives.

Article 10

Règlement des différends

Tout différend entre les États parties, né de l'interprétation ou de l'application de toute disposition de la présente Annexe, est réglé conformément au Protocole sur les règles et procédures relatives au règlement des différends.

Article 11

Révision et modification

La présente Annexe fait l'objet d'une révision et de modification conformément aux articles 28 et 29 de l'Accord sur la ZLECAf, respectivement.

Article 12

Textes authentiques

La présente Annexe est établie en six (6) textes originaux en langues anglaise, arabe, espagnole, française, kiswahili et portugaise, qui font tous également foi.

ANNEXE SUR LES

CRITÈRES DE DÉTERMINATION DES RAISONS LÉGITIMES ET LÉGALES D'INTÉRÊT PUBLIC JUSTIFIANT LA DIVULGATION DU CODE SOURCE

PREMIÈRE PARTIE

DISPOSITIONS GÉNÉRALES

Article premier

Définitions

Aux fins de la présente Annexe, l'on entend par :

a. **« Algorithme »,** un ensemble défini de procédures numériques séquentielles, utilisées pour résoudre un problème particulier ou pour exécuter ou réaliser une tâche particulière ;
b. **« Annexe »**, l'Annexe sur les critères de détermination des raisons légitimes et légales d'intérêt public justifiant la divulgation du code source au Protocole ;
c. **« Personne d'un État partie »,** une personne d'un État partie telle que définie à l'article 1(p) du Protocole ;
d. **« Logiciel »,** un programme ou une série de programmes contenant des instructions destinées à un ordinateur et nécessaires soit au fonctionnement de l'ordinateur lui-même, soit à l'exécution de tâches spécifiques ; et
e. **« Code source »,** un ensemble d'instructions programmées écrites par un programmeur à l'aide d'un langage de programmation spécifique pour exécuter ou réaliser des tâches ou des fonctions particulières, qui est généralement une version lisible par l'homme et qui peut être exécutée par un ordinateur pour former la base d'un logiciel.

Article 2

Objectifs

Les objectifs de la présente Annexe sont :

a. donner effet à l'article 24, alinéa 2, du Protocole ;
b. promouvoir les intérêts publics légitimes et légaux et le transfert de technologie dans la réglementation du commerce numérique sans préjudice des intérêts commerciaux légitimes, de l'innovation technologique, ainsi que de la protection et de l'application des droits de propriété intellectuelle sur le marché numérique de la ZLECAf ; et
c. trouver un équilibre approprié entre les intérêts publics et privés en ce qui concerne le développement socio-économique et technologique.

DEUXIÈME PARTIE

OBJECTIFS LÉGITIMES ET LÉGAUX D'INTÉRÊT PUBLIC

Article 3

Intérêts publics légitimes et légaux

Un organisme de réglementation ou un organe judiciaire d'un État partie peut, conformément à l'alinéa 2 de l'article 24 du Protocole, exiger d'une personne d'un autre État partie ; qu'elle conserve et mette à disposition le code source du logiciel ou un algorithme exprimé dans ce code source, sous réserve des garanties contre la divulgation non autorisée prévues par la législation ou la pratique d'un État partie, afin de poursuivre des objectifs légitimes et légaux d'intérêt public, y compris pour :

a. maintenir l'ordre et la sécurité publics ;
b. protéger la moralité publique ;
c. protéger la vie ou la santé humaine, animale ou végétale ;
d. protéger les intérêts essentiels en matière de sécurité ;
e. protéger les infrastructures critiques et y accéder;
f. prévenir les pratiques trompeuses et frauduleuses ; ou
g. prévenir les discriminations arbitraires ou injustifiables.

TROISIÈME PARTIE

GARANTIES ET PROCÉDURES

Article 4

Garanties

1. Un organisme de réglementation ou une autorité judiciaire d'un État partie, qui exige le transfert d'un code source ou d'un algorithme ou l'accès à ceux-ci en vertu de la présente Annexe, protège le code source du logiciel ou un algorithme exprimé dans ce code source conservé et mis à leur disposition par une personne de l'État partie conformément à l'article 3 de la présente Annexe contre l'accès, l'acquisition ou l'appropriation illicites par un tiers.

2. Un organisme de réglementation ou une autorité judiciaire d'un État partie, qui exige le transfert d'un code source ou d'un algorithme ou l'accès à ceux-ci en vertu de la présente Annexe, n'applique pas l'article 3 de la présente Annexe d'une manière qui :

   a. constitue une restriction déguisée au commerce numérique ou une pratique commerciale malhonnête ;
   b. constitue un moyen de discrimination arbitraire ou injustifiable ;
   c. porte un préjudice injustifié aux intérêts légitimes de la personne concernée d'un État partie ;
   d. est incompatible avec la protection et l'application des droits de propriété intellectuelle sur le marché numérique de la ZLECAf ; ou
   e. restreint le commerce numérique plus que nécessaire pour atteindre des objectifs légitimes et légaux d'intérêt public.

3. Il est entendu que les pratiques commerciales malhonnêtes visées à l'alinéa 2 du présent article comprennent des pratiques telles que la rupture de contrat, l'abus de confiance et l'incitation à la rupture et l'acquisition par des tiers du code source préservé ou disponible d'un logiciel ou d'un algorithme exprimé dans ce code source ou cet algorithme.

4. Il est entendu qu'un tiers visé dans le présent article comprend une personne physique ou morale autre que le propriétaire du code source, y compris une autorité publique, une agence ou un organisme d'un État partie ou d'un tiers tel que défini à l'article 1(u) du Protocole.

Article 5

Cybersécurité

1. Un organisme de réglementation ou une autorité judiciaire d'un État partie, qui exige le transfert d'un code source ou d'un algorithme exprimé dans ce code source ou l'accès à ceux-ci conformément à l'article 3 de la présente Annexe, adopte ou maintient les mesures nécessaires pour protéger ce code source ou cet algorithme contre les fuites de données ainsi que contre la cybercriminalité et les cybermenaces.

2. Un organisme de réglementation ou une autorité judiciaire d'un État partie qui obtient ou demande l'accès à un code source ou à un algorithme exprimé dans ce code source ou l'accès à ceux-ci conformément à l'article 3 de la présente Annexe démontre, auprès de toute autorité compétente convenue par les deux parties, ses compétences en matière de gestion des incidents de cybersécurité, d'atténuation des intrusions malveillantes ou d'utilisation des mécanismes nécessaires pour faire face aux incidents de cybersécurité.

3. Un organisme de réglementation ou une autorité judiciaire d'un État partie qui ne se conforme pas aux obligations visées aux alinéas 1 et 2 du présent article se voit refuser l'accès à un code source ou à un algorithme exprimé dans ce code source.

Article 6

Procédures équitables et raisonnables

1. Lorsqu'un code source ou un algorithme a été demandé et mis à disposition conformément à l'article 3 de la présente Annexe, un organisme de réglementation ou une autorité judiciaire d'un État partie informe, dans un délai de trois (3) mois à compter de la date de soumission du code source ou de l'algorithme exprimé dans ce code source par une personne d'un Etat partie, informer la personne touchée d'un Etat partie de la décision concernant la demande;

2. Chaque État partie adopte ou maintient des procédures transparentes, équitables et raisonnables qui permettent à une personne touchée d'un autre État partie de réexaminer et de contester rapidement et de manière impartiale la décision visée à l'alinéa 1 du présent article et, le cas échéant, de disposer de voies de recours appropriées.

3. Les États parties publient ou rendent publiques sans délai les décisions ou procédures visées dans le présent article, sous réserve des dispositions de l'article 41 du Protocole.

Article 7

Transparence et notification

1. Chaque État partie s'engage dans les meilleurs délais à :

   a. publier ou mettre à la disposition du public dans les meilleurs délais, y compris par des moyens électroniques, ses lois, réglementations, politiques, procédures et décisions

administratives d'application générale qui affectent ou concernent l'obligation d'accéder au code source d'un logiciel ou d'un algorithme exprimé dans ce code source, ou de le transférer ; et

b. notifier aux autres États parties, par l'intermédiaire du Secrétariat, l'introduction de toute nouvelle loi et réglementation, ou de tout amendement à des lois et réglementations en vigueur, ou de toute mesure concernant, affectant ou exigeant l'accès au code source d'un logiciel ou à un algorithme exprimé dans ce code source, ou le transfert de ceux-ci.

2. Aucune disposition du présent article ne peut être interprétée comme obligeant un État partie à divulguer des informations et données confidentielles ou à permettre l'accès à de telles informations et données, dont la divulgation ferait obstacle à l'application des lois ou porterait préjudice aux intérêts commerciaux et stratégiques légitimes d'entreprises ou d'institutions particulières, qu'elles soient publiques ou privées, ou serait de toute autre manière contraire à ses intérêts publics ou essentiels en matière de sécurité.

QUATRIÈME PARTIE

DISPOSITIONS FINALES

Article 8

Règlements et lignes directrices

Les États parties peuvent développer des réglementations ou des lignes directrices continentales sur l'un des aspects de la présente Annexe afin de faciliter sa mise en œuvre et son application effectives.

Article 9

Règlement des différends

Tout différend entre les États parties, né de l'interprétation ou de l'application de toute disposition de la présente Annexe, est réglé conformément au Protocole sur les règles et procédures relatives au règlement des différends.

Article 10

Révision et modification

La présente Annexe fait l'objet d'une révision et d'une modification conformément aux articles 28 et 29 de l'Accord sur ZLECAf.

Article 11

Textes authentiques

La présente Annexe est établie en six (6) textes originaux en langues anglaise, arabe, espagnole, française, kiswahili et portugaise, qui font tous également foi.

ANNEXE SUR LA
SÉCURITÉ ET SÛRETÉ EN LIGNE

Article premier
Définitions

Aux fins de la présente Annexe, l'on entend par :

a. **« Annexe »**, l'Annexe sur la sécurité et la sûreté en ligne du Protocole ;
b. **« Enfant ou mineur »**, tout être humain âgé de moins de 18 ans ;
c. « **Matériel d'abus sexuel d'enfants »,** toute représentation écrite, sonore ou visuelle, y compris toute photographie, film, vidéo ou image, réalisée ou produite par des moyens électroniques, mécaniques ou autres, d'un comportement sexuellement explicite, dans lequel :
   i. la production de cette représentation visuelle implique un enfant;
   ii. une telle représentation visuelle est une image numérique, une image d'ordinateur ou une image générée par ordinateur dans laquelle un enfant se livre à un comportement sexuellement explicite ou dans laquelle des images de ses organes sexuels sont produites ou utilisées à des fins principalement sexuelles et exploitées avec ou sans la connaissance de l'enfant ; et
   iii. une telle représentation visuelle a été créée, adaptée ou modifiée pour donner l'impression qu'un enfant se livre à un comportement sexuellement explicite.

d. **« Autorité compétente »,** un organisme public, une agence, un régulateur ou toute autorité désignée ou habilitée par le droit interne d'un État partie à exécuter et à faire appliquer les mesures relatives à la sécurité et à la sûreté en ligne couvertes par la présente Annexe ;
e. **« Infrastructures critiques »,** les services et installations, y compris les actifs numériques et physiques, les systèmes et les réseaux, qui sont essentiels au bon fonctionnement de l'économie nationale, à la santé publique ou à la sûreté et à la sécurité d'un État partie ;
f. « **Cyberintimidation »,** l'utilisation de moyens électroniques pour harceler, menacer, embarrasser, humilier ou cibler de toute autre manière une autre personne physique **;**
g. **« Plateforme numérique »**, une plateforme numérique définie à l'article 1(c) de l'Annexe sur les Règles d'origine du Protocole ;
h. **« Contenu illégal »**, toute information qui, en elle-même ou en relation avec une activité, y compris la vente de produits ou la prestation de services, enfreint la législation ou les règlements de tout État partie ;
i. **« Menace en ligne »**, toute activité ou tout contenu présentant un risque pour la sécurité en ligne ;
j. **« Personne d'un État partie »**, une personne d'un État partie telle que définie à l'article 1(p) du Protocole ;
k. **« Racisme »,** tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise, encourage ou incite à la haine, à la discrimination ou à la violence à l'encontre d'une personne ou d'un groupe de personnes pour des raisons fondées sur la race, la couleur, l'ascendance, l'origine nationale ou ethnique, ou la religion ; et
l. **« Données à caractère personnel sensibles »**, les données à caractère personnel sensibles telles que définies à l'article 1(k) de l'Annexe sur les transferts transfrontaliers de données du Protocole.

Article 2
Objectifs

Les objectifs de la présente Annexe sont de :

a. donner effet à l'alinéa 2 de l'article 29 du Protocole ;
b. favoriser un environnement en ligne sûr et sécurisé qui soutient le commerce numérique, l'innovation, la croissance et le développement socio-économiques et la protection des droits de l'homme ;
c. renforcer la coopération et la collaboration multipartite entre les États parties, les autorités chargées de l'application de la loi, les régulateurs, le secteur industriel concerné, les consommateurs et la société civile en ce qui concerne la sécurité en ligne et les problèmes de sécurité dans le commerce numérique ; et
d. établir des règles harmonisées prévisibles et transparentes pour la sûreté et la sécurité en ligne dans le commerce numérique.

Article 3
Protection des données à caractère personnel, cybersécurité, protection des consommateurs en ligne et communications électroniques commerciales non sollicitées

Les États parties adoptent ou maintiennent des mesures de protection des données à caractère personnel, et pour assurer la cybersécurité, la protection des consommateurs en ligne et la lutte contre les communications électroniques commerciales non sollicitées, conformément aux articles 21, 25, 27 et 28 du Protocole.

Article 4

Infrastructures critiques

1. Les États parties adoptent ou maintiennent des dispositions législatives et réglementaires pour la maintenance et la protection des infrastructures critiques contre toute perturbation, destruction, ou interférence.

2. Les États parties adoptent une approche fondée sur les risques pour recenser et traiter les infrastructures critiques dans lesquelles un incident de cybersécurité pourrait avoir des effets catastrophiques à l'échelle continentale, régionale, ou nationale sur la santé et la sécurité publiques, la sécurité économique et financière ou les intérêts essentiels en matière de sécurité.

Article 5
Devoir de diligence

1. Chaque État partie adopte ou maintient des lois et réglementations visant à favoriser un environnement en ligne sûr et sécurisé qui soutient le commerce numérique.

2. Chaque État partie exige des entreprises constituées, enregistrées, ou autrement incorporées ou opérant dans sa juridiction qu'elles :

a. se conforment aux lois, réglementations ou mesures applicables en matière de sécurité en ligne ; et
b. adoptent, maintiennent et publient leurs politiques et procédures en matière de sécurité en ligne.

3. Les lois et règlements visés à l'alinéa 1 du présent article exigent notamment des plateformes numériques qu'elles mettent en œuvre les mesures visant à :

a. lutter contre la vente en ligne de contenus, de produits et de services numériques illégaux ;
b. lutter contre l'enregistrement, la vente ou la diffusion en ligne de contenus illégaux et de produits numériques, y compris d'informations et d'images, qui comprennent des propos haineux, des abus sexuels en ligne, du matériel d'abus sexuel d'enfants, des contenus ou matériels pornographiques, la cyberintimidation, et l'incitation à la violence et au racisme ;
c. publier, dans un format lisible par machine et de manière facilement accessible, des lignes directrices sur les contenus interdits, à qui ils sont interdits, sur la manière dont les plaintes sont déposées ou traitées, ainsi que sur les décisions prises et sur la manière dont elles sont prises, et ce, en temps utile, de manière non discriminatoire et non arbitraire ;
d. interdire la publicité ciblée basée sur l'utilisation de données à caractère personnel sensibles et de données personnelles d'enfants ;
e. interdire les interfaces et les pratiques visant à induire les utilisateurs en erreur ; et
f. mettre en place des mesures appropriées pour garantir le plus haut niveau de protection de la vie privée, de la sécurité et de la sûreté des mineurs sur leur service.

4. Les États parties harmonisent leurs lois et règlements relatives à la sécurité et à la sûreté en ligne en tenant compte des normes et pratiques internationales, continentales et régionales.

5. Les États parties font en sorte que les lois et règlements visés au présent article ne soient pas adoptés ou appliqués d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable ou une restriction déguisée au commerce numérique, et à ce qu'ils n'imposent pas au commerce numérique plus de restrictions qu'il n'est nécessaire pour atteindre l'objectif visé.

6. La présente Annexe ne doit pas être appliquée et interprétée comme restreignant les discours protégés par la loi y compris les œuvres ayant une valeur artistique ou d'intérêt pour les médias, tels que les commentaires, les critiques, les satires ou les parodies.

Article 6

Autorités compétentes

1. Chaque État partie établit ou désigne une autorité compétente chargée de faire appliquer les réglementations ou mesures de sécurité en ligne énoncées dans la présente Annexe.

2. Les États parties notifient sans délai, par l'intermédiaire du Secrétariat, les autres États parties de leurs autorités compétentes visées à l'alinéa 1 du présent article.

3. Le Secrétariat met à la disposition du public et communique à tous les États parties les noms et les coordonnées des autorités compétentes désignées par les États parties et chargées de l'application des réglementations en matière de sécurité et de sûreté en ligne dans leurs juridictions respectives.

4. Les États parties font en sorte que leurs autorités compétentes :
a. coopèrent et collaborent avec les autorités compétentes des autres États parties pour répondre aux préoccupations transfrontalières en matière de sécurité et de sûreté en ligne ; et

b. s’acquittent de leurs tâches de manière impartiale, transparente et opportune.

5. Les États parties fournissent à leurs autorités compétentes, dans la mesure de leurs capacités, les ressources nécessaires, notamment les ressources techniques, financières et humaines pour assurer de manière adéquate la sécurité et la sûreté en ligne.

6. Les États parties, en tenant compte des principes de légitimité, de nécessité et de proportionnalité, adoptent ou maintiennent les mesures nécessaires visant à conférer aux autorités compétentes des pouvoirs de blocage, de filtrage et de retrait des contenus illicites sur la base de motifs juridiques déterminés, dans le but d’assurer la sécurité et la sûreté en ligne.

7. Les États parties adoptent ou maintiennent des mesures visant à améliorer et, si nécessaire, établir des canaux de communication entre leurs autorités compétentes afin de faciliter un échange sûr et rapide d’informations concernant tous les aspects de la sécurité et de la sûreté en ligne couverts par la présente Annexe.

Article 7
Transparence et notification

1. Chaque État partie s’engager dans les meilleurs délais à :

a. publier ou mettre à la disposition du public, y compris par des moyens électroniques, ses lois, règlements, politiques, procédures et décisions administratives d’application générale relatifs à la sécurité et à la sûreté en ligne ; et
b. notifier rapidement aux autres États parties, par l’intermédiaire du Secrétariat, l’introduction de toute nouvelle loi ou réglementation ou de tout amendement à des lois et réglementations en vigueur, ou de toutes mesures relatives à la sécurité et à la sûreté en ligne.

2. Aucune disposition du présent article ne peut être interprétée comme obligeant un État partie à divulguer des informations et données confidentielles ou à permettre l’accès à de telles informations et données, dont la divulgation ferait obstacle à l’application des lois ou porterait préjudice aux intérêts commerciaux et stratégiques légitimes d’entreprises ou d’institutions particulières, qu’elles soient publiques ou privées, ou serait de toute autre manière contraire à ses intérêts publics ou essentiels en matière de sécurité.

Article 8
Coopération

1. Les États parties coopèrent entre eux, conformément aux dispositions du présent article et par l’application des instruments internationaux et régionaux pertinents, des arrangements convenus sur la base d’une législation unilatéral ou réciproque et des législations nationales, dans la mesure du possible, aux fins d’enquêtes ou de procédures concernant la sécurité et la sûreté en ligne.

2. Les États parties coopèrent pour faire progresser les solutions de collaboration en matière de sécurité et sûreté en ligne dans le commerce numérique, notamment par les moyens suivants :

a. une approche multipartite impliquant les gouvernements, les autorités chargées de l'application de la loi, le secteur industriel concerné, les consommateurs, la société civile et les communautés techniques ;
b. l'échange de renseignements et de bonnes pratiques ;
c. l'assistance mutuelle dans le cadre d'enquêtes et de poursuites ;
d. des campagnes de sensibilisation du public visant à promouvoir et à améliorer la sécurité en ligne ;
e. la recherche et le développement conjoints d'outils et de technologies de sécurité et sûreté en ligne ; et
f. l'éducation, la formation, et le renforcement des capacités des autorités chargées de l'application de la loi et des autorités judiciaires et des autres parties prenantes concernées.

3. Les États parties collaborent, si nécessaire, avec les organismes régionaux, continentaux, et internationaux compétents pour la mise en œuvre de la présente Annexe.

Article 9

Règlements et lignes directrices

Les États parties peuvent développer des réglementations ou des lignes directrices continentales sur l'un des aspects de la présente Annexe afin de faciliter sa mise en œuvre et son application effectives.

Article 10

Règlement des différends

Tout différend entre les États parties, né de l'interprétation ou de l'application de toute disposition de la présente Annexe, est réglé conformément au Protocole sur les règles et procédures relatives au règlement des différends.

Article 11

Révision et modification

La présente Annexe fait l'objet d'une révision et de modification conformément aux articles 28 et 29 de l'Accord sur la ZLECAf, respectivement.

Article 12

Textes authentiques

La présente Annexe est établie en six (6) textes originaux en langues anglaise, arabe, espagnole, française, kiswahili et portugaise, qui font tous également foi.

ANNEXE SUR LES
TRANSFERTS TRANSFRONTALIERS DE DONNÉES

PREMIÈRE PARTIE

DISPOSITIONS GÉNÉRALES

Article premier

Définitions

Aux fins de la présente Annexe, l'on entend par :

a. **« Annexe »,** l'Annexe sur les transferts transfrontaliers de données du Protocole **;**
b. **« Autorité compétente »,** un organisme public, une agence, un régulateur, ou toute autorité désignée ou habilitée par le droit interne d'un État partie à appliquer et à faire respecter les lois sur la protection des données couvertes par la présente Annexe ;
c. **« Consentement »,** toute indication ou volonté librement consentie, expresse, informée et non équivoque de la personne concernée par laquelle elle accepte ou signifie explicitement son accord pour le transfert ou le traitement de ses données à caractère personnel ;
d. **« Transfert transfrontalier de données »,** le transfert de données, y compris de données à caractère personnel, par voie électronique entre les juridictions des États parties ;
e. **« Données »**, toutes les informations et données, autres que les données à caractère personnel définies à l'article 1(q) du Protocole, requises, stockées, utilisées, traitées ou collectées par une personne d'un État partie ;
f. **« Personne concernée »**, toute personne physique faisant l'objet de données à caractère personnel ;
g. **« Commerce numérique »**, le commerce numérique tel que défini à l'article 1(g) du Protocole ;
h. **« Interopérabilité »,** telle que définie à l'article 1(f), de l'Annexe sur les identités numériques du Protocole ;
i. **« Personne d'un État partie »,** une personne d'un État partie telle que définie à l'article 1(p) du Protocole ;
j. **« Données à caractère personnel » :** les données à caractère personnel telles que définies à l'article 1(q) du Protocole ;
k. **« Traitement des données à caractère personnel »,** toute opération ou tout ensemble d'opérations, ou d'activités effectuées à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou par toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, et le verrouillage, le cryptage, l'effacement ou la destruction de données à caractère personnel ; et
l. **« Données à caractère personnel sensibles »,** toutes les données à caractère personnel relatives à l'origine raciale ou ethnique, aux convictions religieuses ou philosophiques, aux données génétiques, aux données biométriques, aux données financières, aux données relatives à la santé ou aux données relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne physique, ou toute autre donnée à caractère

personnel qui, si elle était divulguée, causerait un préjudice, un dommage ou un préjudice aux droits, aux intérêts ou au bien-être d'une personne physique.

Article 2

Objectifs

Les objectifs de la présente Annexe sont les suivants :

a. donner effet à l'alinéa 3 de l'article 20 du Protocole ;
b. éliminer les obstacles réglementaires et administratifs aux transferts transfrontaliers de données au sein du marché numérique de la ZLECAf ;
c. faciliter les transferts transfrontaliers de données tout en protégeant les données personnelles afin de stimuler le commerce numérique, l'innovation et la croissance socio-économique inclusive au sein du marché numérique de la ZLECAf ;
d. établir des règles harmonisées prévisibles et transparentes, ainsi que des principes et des normes communs pour des transferts de données transfrontaliers sûrs et sécurisés au sein du marché numérique de la ZLECAf ;
e. renforcer la capacité concurrentielle des entreprises des États parties et accélérer leur intégration bénéfique dans le marché numérique mondial ; et
f. favoriser la coopération et la collaboration entre les États parties sur les transferts transfrontaliers de données afin d'atteindre les objectifs de la ZLECAf liés au développement socio-économique durable des économies et des sociétés africaines.

Article 3

Champ d'application

1. La présente Annexe s'applique aux transferts électroniques transfrontaliers de données, y compris de données à caractère personnel, effectués aux fins de commerce numérique par une personne d'un État partie.

2. La présente Annexe ne s'applique pas à ce qui suit :

a. les transferts transfrontaliers de données effectués à des fins qui ne relèvent pas du commerce numérique telles que définies à l'article 1(g) du Protocole ; et
b. les données ou informations détenues ou traitées par un État partie ou pour son compte, ou les mesures relatives à ces données ou informations, y compris les mesures relatives à leur collecte, à l'exception des informations gouvernementales ouvertes prévues à l'article 39 du Protocole.

DEUXIÈME PARTIE

PRINCIPES ET NORMES DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Article 4

Cadres juridiques de protection des données à caractère personnel

1. Conformément à l'alinéa 1 de l'article 21 du Protocole, chaque État partie adopte ou maintient un cadre juridique qui prévoit la protection des données à caractère personnel des personnes physiques qui se livrent au commerce numérique.

2. Les cadres juridiques visés à l'alinéa 1 du présent article sont conformes aux normes énoncés dans les articles 5 à 14 de la présente Annexe.

Article 5
Principes de protection des données personnelles

Les États parties adoptent ou maintiennent, dans leur cadre juridique, les principes fondamentaux suivants en matière de protection des données à caractère personnel :

a. légalité, équité et transparence ;
b. minimisation des données ;
c. limitation de l'objectif ;
d. limitation du stockage ;
e. précision ;
f. sécurité, confidentialité et intégrité ; et
g. responsabilité.

Article 6
Droits des personnes concernées

1. Les États parties prévoient, dans leur cadre juridique :

a. les droits des personnes concernées en ce qui concerne leurs données à caractère personnel, y compris le droit d'accès, de rectification, d'effacement, de portabilité des données, d'opposition au traitement des données à caractère personnel et d'être informée du traitement de leurs données à caractère personnel ; et
b. en sorte qu'une personne d'un État partie impliquée dans le traitement des données à caractère personnel fournisse, de manière transparente et accessible, ses politiques et pratiques en matière de données à caractère personnel, y compris.

i. les données personnelles collectées ;
ii. la finalité de la collecte des données à caractère personnel ;
iii. les personnes auxquelles les données personnelles peuvent être divulguées ;
iv. la période de conservation ; et
v. des informations sur la manière de contacter les personnes au sujet de leurs pratiques et de leur traitement des données à caractère personnel.

Article 7

Minimisation des données

1. Les États parties font, dans leur cadre juridique :

a. en sorte que la collecte de données à caractère personnel soit limitée aux données pertinentes au regard de la finalité de la collecte et à ce que ces données soient obtenues par des moyens licites et loyaux et, le cas échéant, en informant la personne concernée et en obtenant son consentement ;
b. en sorte qu'une personne d'un État partie ne collecte ni ne conserve des données à caractère personnel qui ne sont pas nécessaires à la conduite du commerce numérique, ni ne combine des données à caractère personnel stockées, ou relatives à l'utilisation de données à caractère personnel, provenant de différents services offerts par cette personne ou de services de tiers, qui ne sont pas nécessaires à la conduite du commerce numérique, à moins que la personne concernée n'ait donné son consentement.

Article 8

Mesures de sécurité

Les États parties exigent, dans leur cadre juridique, qu'une personne d'un État partie impliquée dans le traitement de données à caractère personnel protège les données à caractère personnel qu'elle détient au moyen de garanties appropriées contre les risques, y compris, mais sans s'y limiter, le vol ou l'accès non autorisé, la destruction, l'utilisation, la modification, le transfert ou la divulgation de données à caractère personnel, ou d'autres formes d'utilisation abusive.

Article 9

Protection des données à caractère personnel dès la conception et par défaut

Les États parties exigent, dans leur cadre juridique, qu'une personne d'un État partie impliquée dans le traitement de données à caractère personnel protègent ces données à la fois au moment de la détermination des moyens de traitement et au moment du traitement, en incorporant les mesures techniques et organisationnelles appropriées conçues pour mettre en œuvre les principes de protection des données de manière efficace, et intègrent les garanties nécessaires dans le traitement de données à caractère personnel afin de protéger les droits des personnes concernées.

Article 10

Mesures correctives

Les États parties prévoient, dans leur cadre juridique :

a. des mesures correctives appropriées en cas de violation de la protection des données, y compris la réparation et la mise en place d'un mécanisme visant à empêcher que les violations ne se poursuivent, ainsi que d'autres recours pertinents proportionnels à l'ampleur du préjudice réel ou potentiel subi par les personnes concernées du fait de ces violations ; et
b. qu'une personne d'un État partie notifie dans les brefs délais les autorités compétentes visées à l'article 11 de la présente Annexe ainsi que les personnes concernées en cas de violation importante affectant la protection des données à caractère personnel placées sous leur contrôle.

Articles 11

Autorités compétentes

1. Chaque État partie établit ou désigne une autorité compétente chargée de l'application des lois sur la protection des données à caractère personnel.

2. Les États parties notifient, par l'intermédiaire du Secrétariat, les autres États parties de leurs autorités compétentes visées à l'alinéa 1 du présent article.

3. Le Secrétariat met à la disposition du public et communique à tous les États parties les noms et les coordonnées des autorités compétentes des États parties désignées pour faire appliquer leurs lois respectives sur la protection des données à caractère personnel.

4. Les États parties font en sorte que leurs autorités compétentes :

   a. coopèrent et collaborent avec les autorités compétentes des autres États parties pour traiter les violations transfrontalières de la protection des données à caractère personnel ; et

b. s’acquittent de leurs devoirs et responsabilités de manière impartiale, transparente, et en temps voulu.

5. Les États parties fournissent à leurs autorités compétentes, dans la mesure de leurs moyens, toutes les ressources nécessaires, y compris des ressources techniques, financières et humaines pour leur permettre de s’acquitter convenablement de leurs devoirs et responsabilités.

6. Les États parties adoptent ou maintiennent des mesures visant à améliorer et, si nécessaire, à établir des voies de communication entre leurs autorités compétentes afin de faciliter un échange sûr et rapide d’informations concernant tous les aspects de la protection des données à caractère personnel couverts par la présente Annexe.

Article 12

Publication des politiques et procédures

Chaque État partie exige d’une personne d’un État partie impliquée dans le traitement des données à caractère personnel sur son territoire qu’elle adopte ou maintienne et publie ses politiques et procédures relatives à la protection des données à caractère personnel.

Article 13

Partage et divulgation de données à caractère personnel à des tiers

1. Les États parties exigent, dans leur cadre juridique, qu’une personne d’un État partie ne partage ni ne divulgue des données à caractère personnel à un tiers, à moins que :

   a. une notification préalable est adressée à la personne concernée et le consentement a été donné par la personne concernée ou l’autorité compétente de l’État partie ; ou
   b. lorsque la personne concernée en est préalablement informée et que la divulgation est nécessaire à l’exécution d’une obligation contractuelle de la personne concernée.

2. Le tiers auquel des données à caractère personnel ont été partagées ou divulguées conformément à l’alinéa 1 ci-dessus ne partage ni ne divulgue ces données à caractère personnel sans le consentement de la personne concernée ou de l’autorité compétente de l’État partie.

3. Le présent article ne s’applique pas dans les cas où la divulgation à des tiers est nécessaire pour se conformer à une obligation légale ou est prescrite par la loi, notamment à des fins de vérification de l’identité, de prévention, de détection ou d’enquête en matière de cybercriminalité, ainsi que de poursuite et de répression des infractions.

4. Il est entendu que, dans le présent article, un tiers désigne une personne physique ou morale autre que la personne concernée, y compris une autorité publique, une agence ou un organisme d’un État partie ou d’un tiers, tel que défini à l’article 1er, point u), du Protocole.

Article 14

Accès des États parties

1. Un État partie n’exige pas l’accès aux :

a. données à caractère personnel détenues par une personne d'un autre État partie comme condition à la conduite du commerce numérique sur son territoire.
b. données à caractère personnel des personnes concernées d'autres États parties détenues par ses personnes physiques ou morales pratiquant le commerce numérique sur le territoire de ces États parties.

2. Le présent article n'empêche pas un organisme de réglementation ou une autorité judiciaire d'un État partie de demander à une personne d'un autre État partie de mettre les données à caractère personnel à la disposition de l'organisme de réglementation ou de l'autorité judiciaire aux fins d'une enquête, d'une inspection, d'une mesure d'exécution ou d'une procédure judiciaire spécifique, ou lorsque cela est nécessaire pour des raisons d'intérêt public légitimes et légals, sous réserve des garanties contre la divulgation non autorisée de données à caractère personnel prévues par le droit ou la pratique d'un État partie.

3. Les garanties et procédures décrites dans les articles 4, 5 et 6 de l'Annexe sur les critères de détermination des raisons d'intérêt public légitimes et légales de la divulgation du code source du Protocole s'appliquent *mutatis mutandis* à l'alinéa 3 du présent article.

Article 15

Interopérabilité et harmonisation

1. Les États parties favorisent l'interopérabilité de leurs cadres juridiques pertinents afin de faciliter les transferts transfrontaliers de données tout en protégeant les données à caractère personnel.
2. Les États parties peuvent conclure des accords ou des arrangements de partage de données et d'interopérabilité des systèmes de données mutuellement avantageux et réciproques, qui tiennent compte des principes de transparence et de non-discrimination et qui respectent les lois pertinentes des États parties en matière de protection des données ou les principes et normes stipulées dans les articles 5 à 14 de la présente Annexe.
3. Les États parties harmonisent leurs lois sur la protection des données, y compris les questions administratives et procédurales, avec les principes et normes stipulés dans les articles 5 à 14 de la présente Annexe en vue de parvenir à un cadre juridique continental harmonisé pour la protection des données au sein du marché numérique de la ZLECAf.

TROISIÈME PARTIE

FACILITATION DES TRANSFERTS TRANSFRONTALIERS DE DONNÉES

Article 16

Principes applicables aux transferts transfrontaliers de données

1. Conformément à l'alinéa 1 de l'article 20 du Protocole, un État partie, sauf dispositions contraires de la présente Annexe, n'applique pas de mesures qui restreignent le transfert transfrontalier de données, y compris de données à caractère personnel, entre son territoire et le territoire d'un autre État partie si le transfert est effectué aux fins du commerce numérique par une personne d'un autre État partie.

2. Il est entendu que les mesures visées à l'alinéa 1 du présent article comprennent, entre autres, toute interdiction, condition, restriction ou limitation, temporaires ou permanentes, prévues par les lois, règlements, exigences administratives ou pratiques d'un État partie pour le transfert de données, y compris de données à caractère personnel, aux fins de commerce numérique par une personne d'un autre État partie.

3. Les États parties adoptent ou maintiennent des mesures raisonnables et appropriées pour garantir que les transferts transfrontaliers de données, y compris de données à caractère personnel, effectués par des personnes des États parties à des fins de commerce numérique sont ininterrompus et sécurisés.

4. Les États parties s'abstiennent de restreindre les transferts transfrontaliers de données, y compris de données à caractère personnel, effectués par une personne d'un État partie, vers un État partie où il existe un cadre juridique stipulé à l'alinéa 1 de l'article 21 du Protocole et des principes et des normes énoncées dans les articles 5 à 14 de la présente Annexe.

5. Les États parties adoptent ou maintiennent des mesures raisonnables et appropriées pour identifier et supprimer les obstacles aux transferts transfrontaliers de données.

Article 17

Niveau de protection équivalent

Chaque État partie accorde aux données, y compris les données à caractère personnel, transférées par une personne d'un autre État partie, le même niveau de protection qu'il accorde aux données, y compris les données à caractère personnel, de ses propres ressortissants.

Article 18

Non-discrimination

1. Un État partie n'accorde pas un traitement moins favorable aux données, y compris les données à caractère personnel de la personne d'autres États parties qu'il n'accorde aux données similaires, y compris les données à caractère personnel de sa propre personne.

2. Un État partie n'accorde pas un traitement moins favorable aux données, y compris les données à caractère personnel, de la personne d'un autre État partie qu'aux données similaires, y compris les données à caractère personnel des personnes d'autres États parties ou des personnes de tiers.

Article 19

Mécanismes de transfert transfrontalier de données

1. Les États parties facilitent les transferts transfrontaliers de données sûrs et sécurisés en encourageant et en soutenant la mise en place de mécanismes qui tiennent compte des principes de transparence, de non-discrimination, et d'interopérabilité et qui sont conformes aux lois pertinentes des États parties en matière de protection des données ou aux normes stipulées dans la deuxième partie de la présente Annexe, y compris, mais sans s'y limiter :

   a. les centres de données régionaux et les systèmes d'informatique en nuage ;
   b. la création de centres de données ou de sites de reprise après sinistre situés dans les États parties ;
   c. l'élaboration de codes de conduite d'autorégulation spécifiques à chaque secteur ;
   d. des systèmes de certification fondés sur des principes pour les transferts transfrontaliers de données, qui permettent notamment aux autorités compétentes de certifier le respect de la protection des données et de mettre en œuvre un système d'évaluation périodique du respect de la protection des données par les personnes certifiées des États parties ; et
   e. des mécanismes de transfert transfrontalier de données adaptés aux besoins et aux défis des micro, petites et moyennes entreprises, des femmes, des jeunes, des populations autochtones, des communautés rurales et locales, des personnes vivant avec un handicap et d'autres groupes sous-représentés.

2. Les État parties encouragent l'élaboration de mécanismes visant à promouvoir la compatibilité entre leurs différents cadres juridiques. Ces mécanismes peuvent inclure la reconnaissance des résultats réglementaires, qu'ils soient accordés unilatéralement ou par arrangement ou accord mutuel.

3. Les États parties collaborent, si nécessaire, avec les parties prenantes concernées pour élaborer les cadres ou mécanismes visés dans le présent article.

4. Les États parties font en sorte que les mécanismes visés dans le présent article facilitent les transferts transfrontaliers de données responsables et imputables et la protection effective de la vie privée sans créer d'obstacles aux transferts transfrontaliers de données, y compris des charges administratives et bureaucratiques inutiles pour les entreprises et les consommateurs.

Article 20

Transparence et notification

1. Chaque État partie s'engage dans les meilleurs délais à :

   a. publier ou mettre à la disposition du public, y compris par des moyens électroniques, ses lois, règlements, politiques, procédures et décisions administratives d'application générale concernant ou affectant les transferts transfrontaliers de données et la protection des données à caractère personnel ; et

   b. notifier aux autres États parties, par l'intermédiaire du Secrétariat, l'introduction de toute nouvelle loi ou réglementation ou de tout amendement à des lois et réglementations en vigueur, ou de toute mesure concernant ou affectant les transferts transfrontaliers de données et la protection des données à caractère personnel.

2. Aucune disposition du présent article ne peut être interprétée comme obligeant un État partie à divulguer ou à autoriser l'accès à des informations et données confidentielles dont la divulgation ferait obstacle à l'application des lois ou porterait préjudice aux intérêts commerciaux et stratégiques légitimes d'entreprises ou d'institutions particulières, qu'elles soient publiques ou privées, ou serait de toute autre manière contraire à ses intérêts publics ou essentiels en matière de sécurité.

Article 21

Coopération

1. Les États parties coopèrent, entre autres, par les moyens suivants :

   a. partage des informations relatives à la protection des données, y compris, mais sans s'y limiter, des recherches, des enquêtes et des rapports ;
   b. programmes conjoints de promotion, d'éducation, et de formation pour sensibiliser le public et améliorer sa compréhension de la protection des données et du respect des lois et règlements en la matière ;
   c. entreprendre des activités de consultation et de renforcement des capacités en matière de protection des données ;
   d. assistance judiciaire ; et
   e. partage d'expériences sur les techniques d'investigation des violations transfrontalières de la protection des données et les stratégies réglementaires de règlement des différends liées à ces violations, y compris, entre autres, le traitement des plaintes et les mécanismes alternatifs de règlement des différends.

2. Les États parties engagent un dialogue avec les parties prenantes concernées, y compris, mais sans s'y limiter, le secteur industriel, les consommateurs, le monde universitaire, les organismes professionnels et normatifs, afin d'obtenir des informations sur la protection des données et les transferts transfrontaliers de données et de rechercher une coopération en vue de la réalisation des objectifs de la présente Annexe.

3. Les États parties coopèrent pour faciliter les transferts transfrontaliers de données et leur protection en créant un cadre dans lequel les autorités compétentes peuvent, sur une base volontaire, partager des informations et solliciter et fournir une assistance pour les questions liées aux transferts transfrontaliers de données et à la protection des données.

4. Les États parties révisent et mettent à jour périodiquement leurs normes en matière de transfert transfrontalier et de protection des données afin de s'assurer qu'ils sont alignés sur les meilleures pratiques et les progrès technologiques en matière de protection et de transfert des données.

5. Les États parties élaborent des instruments qui facilitent les transferts transfrontaliers de données, y compris, mais sans s'y limiter, des lignes directrices, des recommandations et des normes.

Article 22

Données pour le développement

Conformément à l'alinéa 3 de l'article 20 du Protocole, les États parties, compte tenu de l'importance des données pour le développement :

   a. facilitent la mise en place de méthodes innovantes pour promouvoir les avantages publics en partageant ou en utilisant les données d'une manière qui permette

d'exploiter les données en Afrique afin de réaliser leur valeur socio-économique dans la prise de décision, la planification, le suivi et l'évaluation du secteur public ;

b. soutiennent les capacités en matière de données afin de tirer parti des technologies et des services fondés sur les données pour favoriser le développement durable et profiter aux économies et aux citoyens africains ;
c. tirent parti de modèles commerciaux fondés sur les données qui peuvent favoriser le commerce numérique intra-africain et l'entrepreneuriat fondé sur les données ;
d. promeuvent l'interopérabilité, le partage des données et la réactivité à la demande de données par l'établissement de normes de données ouvertes dans la création de données, qui se conforment aux principes généraux de l'anonymat, de la vie privée, de la sécurité, et de toute considération sectorielle relative aux données, pour faciliter l'accès aux données non personnelles et certaines catégories de données personnelles, par les chercheurs, les innovateurs et les entrepreneurs africains ;
e. promeuvent la recherche, le développement et l'innovation dans divers domaines fondés sur les données ;
f. soutiennent le développement d'infrastructures de données régionales et continentales pour accueillir des technologies avancées basées sur les données, ainsi que l'environnement favorable et le mécanisme de partage des données nécessaires pour faciliter la circulation des données à travers le continent ; et
g. créent un forum continental pour les décideurs africains, les autorités compétentes, les entreprises concernées, et les autres parties prenantes afin d'exploiter les données comme moteur de l'économie et de la société numériques, de faciliter les échanges entre les États parties et de permettre le partage des connaissances sur la création de valeur et l'innovation en matière de données, ainsi que sur les implications de l'utilisation des données pour la protection de la vie privée et la sécurité des personnes des États parties.

QUATRIÈME PARTIE

EXCEPTIONS GÉNÉRALES

Article 23

Application

1. Les exceptions générales prévues dans les articles 24, 25 et 26 de la présente Annexe s'appliquent au transfert transfrontalier de données, y compris de données à caractère personnel.

2. Les États parties font en sorte que les mesures adoptées ou maintenues en vertu des dispositions de la quatrième partie de la présente Annexe ne soient pas appliquées d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable, ou une restriction déguisée au commerce numérique transfrontalier, et à ce qu'elles n'imposent pas aux transferts de données des restrictions supérieures à celles qui sont nécessaires pour atteindre les objectifs de politique générale et protéger les intérêts essentiels en matière de sécurité.

Article 24

Objectifs de politique publique

En vertu de l'alinéa 2 de l'article 20 du Protocole, un État partie peut adopter ou maintenir des mesures incompatibles avec la présente Annexe pour atteindre des objectifs légitimes de politique publique, notamment la protection des intérêts essentiels de sécurité, le maintien de l'ordre et de la sécurité publics et la protection de la moralité et de la santé publiques.

Article 25

Cadre juridique approprié pour la protection des données à caractère personnel

Un État partie peut restreindre le transfert transfrontalier de données, y compris de données à caractère personnel, vers un autre État partie qui ne dispose pas du cadre juridique prévu à l'alinéa 1 de l'article 21 du Protocole et qui ne prévoit pas les principes et normes énoncées aux articles 5 à 14 partie II de la présente annexe.

Article 26

Données à caractère personnel sensibles

1. Un État partie peut imposer des restrictions sur le transfert transfrontalier de données à caractère personnel sensibles.

2. Dans les cas où le transfert transfrontalier de données à caractère personnel sensibles est nécessaire pour faciliter le commerce numérique, l'État partie autorise ces transferts à condition que :

   a. l'État partie destinataire dispose d'un niveau de protection des données équivalent ou comparable à celui prévu par les lois et règlements de l'État partie d'origine et les normes stipulées dans la deuxième partie de la présente Annexe;
   b. le consentement ait été donné par la personne concernée ;
   c. l'autorisation ait été accordée par l'autorité compétente ;
   d. la personne qui transfère les données à caractère personnel sensibles fasse preuve de diligence raisonnable et prenne des mesures raisonnables pour s'assurer que la personne à laquelle les données à caractère personnel sensibles sont transférées protège ces données conformément aux lois de l'État partie et aux normes stipulées dans la deuxième partie de la présente Annexe ; ou
   e. les mesures et procédures de sécurité applicables soient respectées.

3. Les États parties autorisent le transfert de données à caractère personnel sensibles dans les cas suivants :

   a. ces données sont rendues publiques par la personne concernée ;
   b. la personne concernée a donné son consentement au transfert de ces données ;
   c. le transfert de données à caractère personnel sensibles est nécessaire pour protéger les intérêts vitaux de la personne concernée ou de toute autre personne lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement ; ou
   d. le transfert de données à caractère personnel sensibles est nécessaire pour l'établissement, l'exercice ou la défense de droits en justice.

4. Les États parties font en sorte que les mesures et procédures de sécurité applicables aux transferts transfrontaliers de données à caractère personnel sensibles soient raisonnables, transparentes, prévisibles et non discriminatoires.

5. La personne, physique ou morale, à laquelle les données sensibles à caractère personnel ont été transférées ne transmet pas les données à un tiers sans le consentement de la personne concernée ou de l'autorité compétente.

6. Il est entendu qu'un tiers visé à l'alinéa 5 du présent article comprend une personne physique ou morale autre que la personne concernée, y compris une autorité publique, une agence ou un organisme d'un État partie ou d'un tiers tel que défini à l'article premier, point u), du Protocole.

CINQUIÈME PARTIE

DISPOSITIONS FINALES

Article 27

Règlements et lignes directrices

Les États parties peuvent adopter des réglementations ou des lignes directrices continentales sur l'un des aspects de la présente Annexe afin de faciliter sa mise en œuvre et son application effectives.

Article 28

Règlement des différends

Tout différend entre les États parties découlant de l'interprétation ou de l'application de toute disposition de la présente Annexe ou s'y rapportant est réglé conformément au Protocole sur les règles et procédures relatives au règlement des différends.

Article 29

Révision et modification

La présente Annexe fait l'objet d'une révision et de modifications conformément aux articles 28 et 29 de l'Accord sur la ZLECAf, respectivement.

Article 30

Textes authentiques

La présente annexe est établie en six (6) textes originaux en langues anglaise, arabe, espagnole, française, kiswahili et portugaise, qui font tous également foi

ANNEXE SUR LES
TECHNOLOGIES ÉMERGENTES ET AVANCÉES

PREMIÈRE PARTIE
DISPOSITIONS GÉNÉRALES

Article premier
Définitions

Aux fins de la présente annexe, l'on entend par :

a. **« Annexe »,** l'Annexe sur les technologies émergentes et avancées du Protocole ;
b. « **Technologies émergentes et avancées »,** les technologies en développement, nouvelles, ou développées, y compris, mais sans s'y limiter, l'Internet des objets, l'intelligence artificielle, l'apprentissage automatique, la robotique, la 5G, l'impression 3D, l'informatique quantique, la blockchain, la réalité virtuelle et d'autres technologies existantes et futures en rapport avec le commerce numérique ; et
c. **« Personne d'un État partie »,** une personne d'un État partie telle que définie à l'article 1(p) du Protocole.

Article 2
Objectifs

Les objectifs de la présente Annexe sont :

a. donner effet à l'alinéa 3 de l'article 34 du Protocole ;

b. promouvoir la recherche et le développement pour renforcer les capacités et les compétences numériques liées au développement et au déploiement de technologies émergentes et avancées dans le domaine du commerce numérique ;

c. faciliter, promouvoir et favoriser le déploiement et l'utilisation des technologies émergentes et avancées dans le commerce numérique ;

d. favoriser la coopération et la collaboration entre les États parties dans le développement et le déploiement de technologies émergentes et avancées dans le domaine du commerce numérique ;

e. encourager la réglementation des technologies émergentes et avancées d'une manière qui ne crée pas d'obstacles au commerce numérique ; et

f. établir des règles harmonisées prévisibles et transparentes, ainsi que des principes et des normes communs pour l'adoption et la réglementation des technologies émergentes et avancées dans le domaine du commerce numérique.

Article 3
Champ d'application

La présente Annexe s'applique aux technologies émergentes et avancées déployées et utilisées dans le commerce numérique par les ressortissants des États parties.

DEUXIÈME PARTIE

FACILITATION DU DÉPLOIEMENT ET DE L'UTILISATION DES TECHNOLOGIES ÉMERGENTES ET AVANCÉES DANS LE DOMAINE DU COMMERCE NUMÉRIQUE

Article 4

Déploiement et utilisation

1. Les États parties facilitent, encouragent et favorisent le déploiement et l'utilisation des technologies émergentes et avancées dans le domaine du commerce numérique par les ressortissants des États parties, y compris les entreprises à capitaux africains et les plateformes numériques africaines.

2. Les États parties adoptent ou maintiennent des dispositions législatives et réglementaires qui facilitent, encouragent et favorisent le développement, l'accès, le déploiement et l'utilisation de technologies émergentes et avancées dans le domaine du commerce numérique par les ressortissants des États parties, y compris les entreprises appartenant à des Africains et les plateformes numériques africaines.

3. Un État partie ne doit pas refuser à une personne d'un autre État partie de faire du commerce numérique sur son territoire au seul motif que cette personne déploie ou utilise des technologies émergentes et avancées.

Article 5

Non-discrimination

1. Un État partie n'accorde pas aux technologies émergentes et avancées élaborées sur le territoire d' autres États parties un traitement moins favorable que celui qu'il accorde aux technologies émergentes et avancées similaires élaborées sur son territoire.

2. Un État partie n'accorde pas un traitement moins favorable aux technologies émergentes et avancées élaborées sur le territoire d'un autre État partie qu'aux technologies émergentes et avancées similaires élaborées sur le territoire d'autres États parties ou de tiers.

Article 6

Droits de propriété intellectuelle

Les États parties protègent et font respecter les droits de propriété intellectuelle liés aux technologies émergentes et avancées déployées et utilisées dans le commerce numérique, conformément à l'article 17 du Protocole sur les droits de propriété intellectuelle.

Article 7

Protection des données et confidentialité

Les dispositions des articles 20 et 21 du Protocole et les dispositions des articles 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 et 21 de l'Annexe sur les transferts transfrontaliers de données du Protocole s'appliquent mutatis *mutandis* à la présente Annexe.

Article 8

Cybersécurité

Les dispositions de l'article 25 du Protocole s'applique mutatis *mutandis* à la présente Annexe.

Article 9

Recherche et développement

1. Les États parties encouragent la recherche et le développement en matière de technologies émergentes et avancées pour le commerce numérique, notamment, par les moyens suivants :

   a. la mise en place et le renforcement de la coopération et la collaboration entre les parties prenantes concernées, y compris les gouvernements, le secteur industriel concerné, les consommateurs et les universités, en matière de recherche et de développement dans le domaine des technologies émergentes et avancées ;
   b. l'amélioration des capacités financières, technologiques et de développement des ressources humaines pour la recherche et le développement dans les technologies émergentes et avancées ;
   c. l'élaboration des cadres réglementaires qui favorisent la recherche et le développement dans les technologies émergentes et avancées ;
   d. la promotion et la facilitation des investissements publics et privés dans la recherche et le développement, en mettant l'accent sur l'innovation et les jeunes pousses dans les technologies émergentes et avancées ; et
   e. l'établissement des institutions continentales, régionales et nationales pour l'innovation numérique et la recherche et le développement afin d'assurer un déploiement et une utilisation efficaces des technologies émergentes et avancées dans le commerce numérique.

2. Les États parties conviennent d'adopter des mesures qui renforcent la participation des entreprises africaines, y compris les micro, petites et moyennes entreprises, les femmes, les jeunes, les personnes vivant avec un handicap, les populations autochtones, les communautés rurales et locales, et les autres groupes sous-représentés aux activités de recherche, de technologie, et d'innovation liées aux technologies émergentes et avancées.

Article 10

Bacs à sable réglementaires

1. Les États parties s'efforcent de mettre en place des bacs à sable réglementaires au niveau national pour faciliter le développement et l'expérimentation de technologies émergentes et avancées sous contrôle réglementaire.

2. Les États parties font en sorte que les bacs à sable réglementaires :

   a. fournissent un environnement contrôlé qui favorise l'innovation et facilite le développement, la formation, l'essai et la validation des cas d'utilisation des technologies émergentes et avancées pendant une période limitée avant leur déploiement et leur utilisation dans le commerce numérique ou leur entrée sur le marché numérique de la ZLECAf ; et
   b. permettent de tester des technologies émergentes et avancées dans des conditions réelles pendant une période limitée.

3. Les États parties collaborent, si nécessaire, pour mettre en place des bacs à sable réglementaires au niveau continental ou régional pour faciliter le développement et l'expérimentation de technologies émergentes et avancées par les ressortissants des États parties, y compris les entreprises d'origine africaine.

Article 11
Cadres de suivi, d'évaluation et d'établissement de rapports

Les États parties peuvent élaborer des cadres de suivi, d'évaluation, et d'établissement de rapports avec des indicateurs et des outils appropriés pour suivre les performances des technologies émergentes et avancées déployées et utilisées dans le commerce numérique.

TROISIÈME PARTIE

NORMES ET RÉGLEMENTATIONS TECHNIQUES

Article 12
Principes d'élaboration des normes techniques et des règlements

1. Les États parties adoptent ou maintiennent des normes et réglementations techniques afin de garantir que les technologies émergentes et avancées sont déployées et utilisées dans le commerce numérique d'une manière sûre, responsable et éthique.

2. Les États parties font en sorte que les réglementations et les normes visées dans le présent article ne soient pas adoptées ou appliquées d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable ou une restriction déguisée au commerce numérique, et n'imposent pas de restrictions au déploiement et à l'utilisation de technologies émergentes et avancées plus importantes que celles qui sont nécessaires pour atteindre l'objectif.

3. Les États parties s'engagent à :

   a. harmoniser leurs normes et réglementations techniques sur le déploiement et l'utilisation des technologies émergentes et avancées dans le commerce numérique ; et
   b. encourager l'interopérabilité des normes et réglementations techniques pour les technologies émergentes et avancées afin de faciliter le commerce numérique.

4. Les États parties s'efforcent, lors de l'adoption ou de la mise à jour de leurs normes et réglementations techniques relatives aux technologies émergentes et avancées, de solliciter et de prendre en compte les contributions de l'industrie concernée, des sociétés techniques et professionnelles, des organismes de normalisation, et d'autres parties prenantes concernées.

5. Lorsqu'ils adoptent ou maintiennent les normes et règlements techniques visés au présent article, les États parties :

   a. prendre en considération les normes, principes et lignes directrices régionaux, continentaux, et internationaux ;
   b. adoptent une approche fondée sur les risques ou toute autre approche pertinente, y compris des processus transparents d'évaluation, de gestion et d'atténuation des

risques associés à des technologies émergentes et avancées spécifiques déployées et utilisées dans le cadre du commerce numérique ;

c. évaluent si les risques potentiels peuvent être atténués ou traités à l'aide des instruments et des cadres réglementaires en vigueur ;
d. examinent si toute réglementation nouvelle ou proposée est proportionnée en mettant en balance les inconvénients potentiels et les avantages économiques et sociaux ;
e. utilisent les meilleures pratiques en matière de gestion des risques, notamment en examinant l'impact de la substitution des risques d'une technologie émergente et avancée spécifique par rapport à un scénario dans lequel une telle technologie n'a pas été déployée, mais où les risques de base demeurent en place ; et
f. promeuvent l'élaboration de normes volontaires pour gérer les risques associés aux technologies émergentes et avancées d'une manière qui soit adaptable aux exigences des technologies dynamiques et évolutives.

6. Les États parties révisent et mettent régulièrement à jour leurs normes et réglementations techniques relatives au déploiement et à l'utilisation des technologies émergentes et avancées, selon les besoins, afin de suivre l'évolution technologique.

QUATRIÈME PARTIE
EXCEPTIONS GÉNÉRALES, TRANSPARENCE, NOTIFICATION ET COOPÉRATION

Article 13
Exceptions générales

Aucune disposition de la présente Annexe n'est interprétée comme empêchant un État partie d'adopter ou de maintenir des mesures incompatibles avec les dispositions de la présente Annexe pour atteindre un objectif légitime de politique publique, notamment pour protéger la sécurité, la santé et le bien-être publics, protéger les intérêts essentiels en matière de sécurité, empêcher les pratiques trompeuses et frauduleuses, et protéger l'environnement, à condition que les mesures ne soient pas appliquées d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable ou une restriction déguisée au commerce numérique, et qu'elles n'imposent pas de restrictions au déploiement et à l'utilisation de technologies émergentes et avancées supérieures à celles qui sont nécessaires pour atteindre l'objectif visé.

Article 14
Transparence et notification

1. Chaque État partie s'engage dans les meilleurs délais à :

a. publier ou mettre à la disposition du public dans les meilleurs délais, y compris par des moyens électroniques, ses lois, règlements, politiques, procédures et décisions administratives d'application générale concernant le déploiement et l'utilisation des technologies émergentes et avancées dans le domaine du commerce numérique ; et
b. notifier rapidement aux autres États parties, par l'intermédiaire du Secrétariat, l'introduction de toute nouvelle loi ou réglementation, de tout amendement à des lois et réglementations en vigueur, ou de toute mesure concernant ou affectant le déploiement et l'utilisation de technologies émergentes et avancées dans le domaine du commerce numérique.

2. Aucune disposition du présent article ne peut être interprétée comme obligeant un État partie à divulguer ou à autoriser l'accès à des informations et données confidentielles

dont la divulgation ferait obstacle à l'application des lois ou porterait préjudice aux intérêts commerciaux et stratégiques légitimes d'entreprises ou d'institutions particulières, qu'elles soient publiques ou privées, ou serait de toute autre manière contraire à ses intérêts publics ou essentiels en matière de sécurité.

Article 15

Coopération

1. Les États parties coopèrent par l'échange de renseignements, de connaissances et d'expertise, la recherche et le développement, les activités de formation, l'apprentissage en équipe, l'assistance technique, la collaboration entre les secteurs public et privé, le renforcement des capacités et le partage d'expériences et de bonnes pratiques en ce qui concerne l'adoption et la réglementation des technologies émergentes et avancées dans le domaine du commerce numérique.

2. Les États parties collaborent, si nécessaire, avec les organismes régionaux, continentaux et internationaux compétents, au développement, à la promotion, à la facilitation, au déploiement et à l'utilisation de technologies émergentes et avancées dans le domaine du commerce numérique, ainsi qu'à la mise en œuvre de la présente Annexe.

CINQUIÈME PARTIE

DISPOSITIONS FINALES

Article 16

Règlements et lignes directrices

Les États parties peuvent développer des règlements et des lignes directrices sur l'un quelconque des aspects de la présente Annexe afin de faciliter sa mise en œuvre et son application effectives.

Article 17

Règlement des différends

Tout différend entre les États parties, né de l'interprétation ou de l'application de toute disposition de la présente Annexe, est réglé conformément au Protocole sur les règles et procédures relatives au règlement des différends

Article 18

Révision et modification

La présente Annexe fait l'objet d'une révision et de modification conformément aux articles 28 et 29 de l'Accord sur la ZLECAf, respectivement.

Article 19

Textes authentiques

La présente annexe est établie en six (6) textes originaux en langues anglaise, arabe, espagnole, française, kiswahili et portugaise, qui font tous également foi.

ANNEXE

SUR LES IDENTITÉS NUMÉRIQUES

PREMIÈRE PARTIE

DISPOSITIONS GÉNÉRALES

Article premier

Définitions

Aux fins de la présente Annexe, l'on entend par :

a. « **Identité numérique ZLECAf** » désigne une identité numérique établie conformément à l'article 13 de la présente Annexe ;
b. **« Annexe »**, l'Annexe sur les identités numériques du Protocole ;
c. **« Authentification »,** le processus ou l'acte consistant à vérifier l'identité numérique d'une personne physique ou morale ;
d. **« Procédure d'évaluation de la conformité** », toute procédure utilisée, directement ou indirectement, pour déterminer si les exigences pertinentes des règlements techniques ou des normes sont remplies ;
e. « **Identité numérique »,** l'identité numérique telle que définie à l'article 1(f) du Protocole ;
f. **« Interopérabilité »,** la capacité de différents systèmes, réglementations, réseaux, bases de données, dispositifs ou applications à communiquer, à exécuter des programmes ou à transférer des données ;
g. **« Données à caractère personnel »,** les données à caractère personnel telles que définies à l'article 1(q) du Protocole ;
h. **« Personne d'un État partie »**, une personne d'un État partie telle que définie à l'article 1(p), du Protocole ;
i. **« Norme »,** un document approuvé par un organisme reconnu, qui fournit, pour un usage commun et répété, des règles, des lignes directrices ou des caractéristiques pour des produits ou des processus et des méthodes de production connexes, dont le respect n'est pas obligatoire ; et
j. **« Règlement technique »,** un document qui définit les caractéristiques d'un produit ou les procédés et méthodes de production qui s'y rapportent, y compris les dispositions administratives applicables, et dont le respect est obligatoire.

Article 2

Objectifs

Les objectifs de la présente Annexe sont de :

a. donner effet à l'alinéa 2 de l'article 14 du Protocole ;
b. soutenir l'interopérabilité transfrontalière, la reconnaissance mutuelle et l'authentification des identités numériques entre les États parties ;
c. faciliter la conduite des affaires, y compris la circulation des personnes physiques et morales au sein de la ZLECAf ;
d. promouvoir l'inclusion numérique, financière et socio-économique au sens large ; et

e. renforcer la confiance et la sécurité dans le commerce numérique dans le cadre de la ZLECAf.

Article 3

Champ d'application

La présente Annexe s'applique aux systèmes d'identité numérique adoptés ou maintenus par les États parties conformément à l'alinéa 1 de l'article 14 du Protocole.

DEUXIÈME PARTIE

OBLIGATIONS DES ÉTATS PARTIES

Article 4
Systèmes d'identité numérique

1. En vertu de l'alinéa 1 de l'article 14 du Protocole, les États parties adoptent ou maintiennent des systèmes d'identité numérique pour les personnes physiques et morales conformément à leurs lois et réglementations.

2. Les États parties font en sorte que les systèmes d'identité numérique visés à l'alinéa 1 du présent article comprennent l'inscription, la délivrance et la gestion des justificatifs d'identité numérique.

3. Les États parties adoptent ou maintiennent des systèmes d'identité numérique dotés de caractéristiques et de facteurs d'authentification robustes qui peuvent inclure, sans s'y limiter, la biométrie, les signatures, les facteurs de forme physique, les codes PIN, les formats numériques, les portails en ligne, les numéros identifiants uniques, les images et les authentifications multi-facteurs telles que le mot de passe à usage unique, en tenant compte des normes régionales, continentales et internationales pertinentes.

Article 5

Authentification

Les États parties prévoient des mécanismes de validation et d'authentification des identités numériques qui peuvent inclure :

a. l'authentification basée sur le web ;
b. l'authentification basée sur l'interface de programmation d'applications ;
c. l'authentification multifactorielle ;
d. l'authentification basée sur un certificat ; ou
e. tout autre mécanisme de validation et d'authentification reconnu.

Article 6

Notification des systèmes d'identité numérique et des autorités de délivrance

1. Chaque État partie notifie sans délai aux autres États parties, par le truchement du Secrétariat, ses systèmes d'identité numérique et les autorités compétentes chargées de délivrer les identités numériques des personnes physiques et morales relevant de sa juridiction.

2. Le Secrétariat établit et tient à jour une base de données des systèmes d'identité numérique des États parties et de leurs autorités émettrices respectives. .

3. Lorsqu'un ou plusieurs États parties ont des préoccupations concernant le système d'identité numérique notifié ou mis en œuvre par un autre État partie, l'État partie ou les États parties concernés peuvent demander, par l' intermédiaire du Secrétariat, les informations ou les consultations nécessaires avec l'autre État partie. Les dispositions pertinentes de l'article 40 du Protocole s'appliquent à la mise en œuvre du présent alinéa.

4. Un État partie notifie sans délai aux autres États parties, par l'intermédiaire du Secrétariat, toute atteinte ou menace à la sécurité, perte d'intégrité ou indisponibilité de son système d'identité numérique, ou la probabilité d'une telle atteinte ou menace, ayant, ou pouvant avoir un impact significatif sur ses systèmes d'identité numérique. Cet État partie prend dans les meilleurs délais les mesures appropriées pour atténuer cette violation, cette menace, cette perte, ou cette probabilité.

Article 7
Non-discrimination

1. Un État partie n'accorde pas un traitement moins favorable aux identités numériques des autres États parties qu'à ses propres identités numériques similaires.

2. Un État partie n'accorde pas un traitement moins favorable aux identités numériques d'autres États parties qu'aux identités numériques similaires d'autres États parties ou de tiers.

Article 8

Niveau de protection comparable et équivalent

1. Chaque État partie accorde aux identités numériques délivrées par d'autres États parties un niveau de protection comparable à celui qu'il accorde à ses propres identités numériques.

2. Les États parties assurent à l'identité numérique des personnes qui se livrent au commerce numérique une protection équivalente à celle prévue pour d'autres formes d'identité délivrées en vertu de leurs lois ou réglementations.

Article 9

Protection des données et confidentialité

Les dispositions des articles 20, 21 et 25 du Protocole et des dispositions des articles 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 et 21 de l'Annexe sur les transferts transfrontaliers de données du Protocole s'appliquent *mutatis mutandis* à la présente Annexe.

TROISIÈME PARTIE

RÉGLEMENTATIONS ET NORMES TECHNIQUES

Article 10

Principes d'élaboration des règlements techniques, des normes et des procédures d'évaluation de la conformité

1. Les États parties font en sorte que les règlements techniques, les normes et les procédures d'évaluation de la conformité relatifs aux identités numériques ne soient pas élaborés, adoptés, ou appliqués d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable, ou une restriction déguisée au commerce numérique, et à ce qu'ils n'imposent pas à l'utilisation des identités numériques des restrictions plus importantes que celles qui sont nécessaires pour atteindre l'objectif visé.

2. Lorsqu'ils adoptent des règlements techniques, des normes et des procédures d'évaluation de la conformité concernant les identités numériques, les États parties prennent en considération les normes, principes et lignes directrices régionaux, continentaux et internationaux pertinents.

3. Les États parties harmonisent leurs règlements techniques, leurs normes et leurs procédures d'évaluation de la conformité relatives aux identités numériques afin de faciliter le commerce numérique.

4. Les États parties favorisent l'interopérabilité des règlements techniques, des normes et des procédures d'évaluation de la conformité relatives aux identités numériques afin de faciliter le commerce numérique.

5. Les États parties s'efforcent, lorsqu'ils adoptent ou maintiennent des règlements techniques, des normes et des procédures d'évaluation de la conformité concernant les identités numériques, de solliciter et d'examiner les contributions de l'industrie concernée, des sociétés techniques et professionnelles compétentes, des organismes de normalisation et des autres parties prenantes concernées.

6. Les États parties réexaminent et mettent régulièrement à jour leurs règlements techniques, normes et procédures d'évaluation de la conformité relatives aux identités numériques, en fonction des avancées technologiques.

Article 11

Reconnaissance mutuelle

1. Les États parties reconnaissent la validité juridique des identités numériques délivrées par les autorités compétentes des autres États parties.

2. Les États parties adoptent des mécanismes de certification et des disciplines pour la reconnaissance mutuelle des identités numériques, sous réserve que les conditions suivantes soient remplies :

   a. le système d'identité numérique est notifié conformément à l'article 6 de la présente Annexe ;
   b. le système d'identité numérique doit être interopérable avec les systèmes des autres États parties conformément aux principes énoncés à l'article 12 de la présente Annexe ; et

c. le niveau d'assurance associé à l'identité numérique doit être adapté au cas d'utilisation prévu. Les États parties peuvent convenir d'un cadre commun pour les niveaux d'assurance ou reconnaître leurs cadres nationaux respectifs, à condition qu'ils offrent des niveaux d'assurance équivalents.

3. Les États parties peuvent procéder à des évaluations conjointes de leurs systèmes d'identité numérique respectifs afin de vérifier qu'ils respectent les conditions de la reconnaissance mutuelle.

4. Les États parties établissent, le cas échéant, une liste de confiance des systèmes d'identité numérique reconnus qui remplissent les conditions de reconnaissance mutuelle établies dans le présent article.

5. Un État partie peut refuser de reconnaître une identité numérique délivrée par un autre État partie s'il est prouvé que les conditions de la reconnaissance mutuelle ne sont pas remplies, à condition que l'État partie qui refuse fournisse une explication et une justification claires de cette décision.

Article 12

Interopérabilité

Les États parties favorisent l'interopérabilité des technologies et des applications pour les identités numériques en adoptant des principes ou des spécifications techniques communes comprenant, mais sans s'y limiter, des normes ouvertes, des enregistrements signés numériquement, des horodateurs, des pistes d'audit sécurisée, des communications sécurisées, la souveraineté des données, la confidentialité par conception ou toutes autres caractéristiques clés pertinentes.

Article 13

Identité numérique de la ZLECAf

1. Les États parties établissent une Identité numérique de la ZLECAf pour faciliter la circulation des personnes physiques et morales qui font des affaires dans le cadre de la ZLECAf, en tenant compte des caractéristiques stipulées à l'article 4 de la présente Annexe.

2. L'Identité numérique de la ZLECAf visée à l'alinéa 1 du présent article est acceptée volontairement par les États parties et est délivrée par la ou les institutions africaines désignées par les États parties participants. Cette (ces) institution(s) doi(ven)t, lors du développement de l'Identité numérique de la ZLECAf, se conformer aux lois et règlements applicables, aux exigences en matière de confidentialité et de sécurité des données et aux dispositions relatives à l'élaboration de règlements techniques, de normes et de procédures d'évaluation de la conformité énoncées dans la présente Annexe et dans d'autres dispositions pertinentes du Protocole.

3. Les institutions africaines chargées de délivrer l'identité numérique de la ZLECAf, ainsi que les règlements et procédures relatives à l'administration et au fonctionnement de l'identité numérique de la ZLECAf sont déterminées par le Conseil des ministres.

Article 14

Transparence et notification

1. Chaque État partie s'engage dans les meilleurs délais à :

   a. publier ou mettre à la disposition du public, y compris par des moyens électroniques, ses lois, règlements, politiques, procédures et décisions administratives d'application générale affectant les identités numériques ou s'y rapportant ;et
   b. notifier aux autres États parties, par l'intermédiaire du Secrétariat, l'introduction de toute nouvelle loi ou réglementation, de tout amendement à des lois et réglementations en vigueur, ou de toute mesure concernant ou affectant l'identité numérique.

2. Aucune disposition du présent article ne peut être interprétée comme obligeant un État partie à divulguer ou à autoriser l'accès à des informations et données confidentielles dont la divulgation ferait obstacle à l'application des lois ou porterait préjudice aux intérêts commerciaux et stratégiques légitimes d'entreprises ou d'institutions particulières, qu'elles soient publiques ou privées, ou serait de toute autre manière contraire à ses intérêts publics ou essentiels en matière de sécurité.

Article 15

Coopération

1. Les États parties coopèrent par :

   a. l'échange de renseignements, de connaissances et d'expertise, la recherche et le développement, les activités de formation, l'apprentissage par les pairs et le partage d'expériences et de bonnes pratiques concernant les politiques et réglementations en matière d'identité numérique, l'assistance technique, la mise en œuvre technique et les normes de sécurité ;
   b. le biais de programmes conjoints de promotion, d'éducation et de formation afin de sensibiliser le public et d'améliorer sa compréhension de l'identité numérique et du respect des lois et réglementations en matière de protection des données ; et
   c. la création d'un cadre dans lequel leurs autorités compétentes respectives peuvent, sur une base volontaire, partager des informations et demander et fournir une assistance pour les questions liées à l'utilisation transfrontalière des identités numériques.

2. Les États parties engagent un dialogue avec les parties prenantes concernées, y compris, mais sans s'y limiter, le secteur industriel, les consommateurs, le monde universitaire et les organismes professionnels et les organismes de normalisation, sur les questions relatives aux identités numériques.

3. Les États parties collaborent, si nécessaire, avec les organismes régionaux, continentaux et internationaux compétents pour le développement des identités numériques et la mise en œuvre de la présente Annexe.

QUATRIÈME PARTIE

DISPOSITIONS FINALES

Article 16

Règlements et lignes directrices

Les États parties peuvent développer des réglementations ou des lignes directrices continentales sur l'un des aspects de la présente Annexe afin de faciliter sa mise en œuvre et son application effectives.

Article 17

Règlement des différends

Tout différend entre les États parties, né de l'interprétation ou de l'application de toute disposition de la présente Annexe, est réglé conformément au Protocole sur les règles et procédures relatives au règlement des différends.

Article 18

Révision et modification

La présente Annexe fait l'objet d'une révision et de modifications conformément aux articles 28 et 29 de l'Accord sur la ZLECAf, respectivement.

Article 19

Textes authentiques

La présente Annexe est établie en six (6) textes originaux en langues anglaise, arabe, espagnole, française, kiswahili et portugaise, qui font tous également foi.

ANNEXE

SUR LES PAIEMENTS NUMÉRIQUES TRANSFRONTALIERS

PREMIÈRE PARTIE

DISPOSITIONS GÉNÉRALES

Article premier

Définitions

Aux fins de la présente Annexe, l'on entend par :

a. **« Monnaie locale africaine »,** une forme de monnaie émise par la banque centrale ou l'autorité monétaire en vertu des lois et règlements d'un État partie en tant que moyen d'échange sur le territoire de cet État partie **;**
b. **« Annexe »**, l'Annexe sur les paiements numériques transfrontaliers du Protocole ;
c. **« Monnaie numérique »**, une monnaie sous forme numérique, y compris, mais sans s'y limiter, les cryptomonnaies, basées sur la technologie des registres distribués, les monnaies numériques des banques centrales, les monnaies fiduciaires numériques et toutes les variantes, y compris les pièces de monnaie stables ;
d. **« Paiement numérique »,** un paiement numérique tel que défini à l'article 1(f) du Protocole ;
e. **« Technologie financière »**, telle que définie à l'article 1, (b), de l'Annexe sur la technologie financière du Protocole ; et
f. **« Personne d'un État partie »,** une personne d'un État partie telle que définie à l'article 1(p) du Protocole.

Article 2

Objectifs

Les objectifs de la présente Annexe sont de :

a. donner effet à l'alinéa 3 de l'article 15 du Protocole ;
b. promouvoir le développement de systèmes numériques de paiements et de règlement transfrontaliers abordables, en temps réel, sûrs, inclusifs, responsables, et universellement accessibles, afin de stimuler le commerce intra-africain ;
c. établir des règles harmonisées prévisibles et transparentes, ainsi que des principes et des normes communs pour les systèmes de paiements et de règlement numériques transfrontaliers au sein de la ZLECAf ;
d. promouvoir l'interopérabilité entre les différents systèmes numériques de paiement et de règlement des États parties ;
e. promouvoir l'utilisation des monnaies locales africaines dans les systèmes de paiement et de règlement numériques transfrontaliers au sein de la ZLECAf ; et
f. faciliter la réalisation de l'objectif du Traité instituant la Communauté économique africaine de créer l'Union monétaire africaine, la Banque centrale africaine et la monnaie unique africaine.

Article 3

Champ d'application

1. La présente Annexe s'applique aux paiements numériques transfrontaliers, de gros ou de détail, effectués par une personne d'un État partie lorsque les instruments et canaux de paiement comprennent, sans s'y limiter, les virements, les transferts électroniques

de fonds, l'argent mobile, les applications mobiles, les codes de réponse rapide, les portefeuilles numériques et les cartes de crédit, de débit et prépayées, et qu'ils sont pris en charge par des systèmes de paiement et de règlement reconnus ou adoptés par les États parties à l'échelle continentale, régionale, et nationale.

2. La présente Annexe s'applique aux systèmes de paiement numérique reconnus et exploités conformément aux lois et réglementations des États parties.

3. Le présent Annexe ne s'applique pas à ce qui suit :

   a. paiements numériques nationaux ou les transactions qui sont initiées et terminées dans un État partie, même si les transactions de paiement sont facilitées par une contrepartie internationale ;
   b. paiements effectués exclusivement en espèces ; et
   c. paiements effectués au moyen de chèques sur support papier, de bons sur support papier, de chèques de voyage sur support papier et de mandats postaux sur support papier.

4. La présente Annexe ne déroge pas aux droits et obligations des États parties en vertu du Protocole sur le commerce des services et ne les modifie pas. Il est entendu qu'en cas de conflit ou d'incohérence entre la présente annexe et le protocole sur le commerce des services, les dispositions du Protocole sur le commerce des services prévalent dans la mesure du conflit ou de l'incohérence.

DEUXIÈME PARTIE

PROMOTION DES PAIEMENTS NUMÉRIQUES

Article 4

Cadre réglementaire favorable

1. Chaque État partie adopte ou maintient un cadre juridique et réglementaire pour les paiements numériques qui, entre autres, n'établit pas de discrimination arbitraire ou injustifiée entre les institutions financières et les autres prestataires de services de paiement, y compris les technologies financières et les opérateurs de réseaux mobiles en ce qui concerne l'accès aux services et à l'infrastructure ainsi que toute prise de décision nécessaire au fonctionnement des systèmes de paiement numérique.

2. Les États parties s'efforcent, dans leur cadre juridique et réglementaire visé à l'alinéa 1 du présent article, de permettre aux prestataires de services de paiement numérique, y compris les entreprises de technologie financière, les détaillants et les opérateurs de réseaux mobiles, d'émettre des instruments et des canaux de paiement numérique et de fournir des services de paiement numérique directement et de manière indépendante, sans devoir s'associer à une institution financière.

Article 5

Concurrence et innovation

1. Les États parties facilitent l'innovation et la concurrence dans le domaine des paiements numériques en permettant l'introduction de nouveaux produits et services financiers et de paiement numérique, par l'adoption de bacs à sable réglementaires et technologiques.

2. Les États parties élaborent des réglementations qui favorisent la concurrence et l'innovation dans le secteur des paiements numériques.

3. Les États parties encouragent l'adoption et l'utilisation de technologies émergentes et avancées ainsi que de méthodes et de plateformes de paiement telles que l'argent mobile, l'argent électronique, les monnaies numériques des banques centrales, les interfaces de programmation d'applications et les technologies de réglementation et de surveillance afin de promouvoir des paiements numériques inclusifs, efficaces, efficients, sûrs et durables, sous réserve des dispositions de l'Annexe sur les technologies émergentes et avancées et de l'Annexe sur les technologies financières du Protocole, et en collaboration avec les entreprises, les banques centrales, et les organismes de normalisation compétents.

4. Les États parties accélèrent l'adoption et l'utilisation des paiements numériques, notamment, par les moyens suivants :

   a. faciliter la fourniture de produits et de services de paiement numérique innovants, rapides et peu coûteux, tels que les paiements instantanés, la monnaie électronique et l'argent mobile ;
   b. permettre les paiements numériques pour les paiements de détail hors ligne ; et
   c. promouvoir la connaissance des paiements numériques et la sensibilisation des micro, petites et moyennes entreprises africaines, des femmes, des jeunes, des populations autochtones, des communautés rurales et locales, des personnes handicapées et d'autres groupes sous-représentés.

Article 6

Monnaies numériques

1. Les États parties, conformément à leurs lois et réglementations nationales, adoptent ou maintiennent les monnaies numériques comme moyen d'échange dans leurs juridictions afin, entre autres, de faciliter les paiements numériques transfrontaliers pour le commerce intra-africain.

2. Les États parties qui ont adopté ou maintenu les monnaies numériques comme moyen d'échange conformément à l'alinéa 1 du présent article peuvent conclure des accords ou des arrangements sur les monnaies numériques afin de faciliter les paiements numériques transfrontaliers pour le commerce intra-africain.

Article 7

Monnaies locales africaines

1. Les États parties promeuvent l'utilisation des monnaies locales africaines dans l'opérationnalisation des systèmes numériques transfrontaliers de paiement et de règlement afin de stimuler le commerce intra-africain.

2. Les États parties coopèrent pour promouvoir la convertibilité des monnaies locales afin de renforcer le commerce intra-africain et de réduire les coûts de transaction des paiements numériques transfrontaliers.

3. Les États parties peuvent conclure des accords ou des arrangements sur une monnaie unique ou des monnaies librement convertibles pour les paiements numériques, à condition que la monnaie librement convertible soit une monnaie locale africaine ou toute autre monnaie africaine introduite par de tels accords ou arrangements.

4. Les États parties qui sont parties aux accords ou arrangements visés à l'alinéa 3 du présent article s'engage à :

a. donner aux autres États parties intéressés la possibilité de négocier l'adhésion à ces accords ou arrangements ; et
b. informer sans délai, par le truchement du Secrétariat, les autres États parties de l'ouverture de négociations sur ces accords ou arrangements afin de donner à tout autre État partie ou à tous autres États parties la possibilité de manifester leur intérêt à participer aux négociations avant qu'elles n'entrent dans une phase de fond.

TROISIÈME PARTIE

FACILITATION DES PAIEMENTS NUMÉRIQUES TRANSFRONTALIERS

Article 8

Non-discrimination

1. Un État partie n'accorde pas à un système de paiement et de règlement numérique ou à un instrument de paiement d'un autre État partie un traitement moins favorable qu'à un système de paiement et de règlement numérique ou à un instrument de paiement similaire de son propre État.

2. Un État partie n'accorde pas à un système de paiement et de règlement numérique ou à un instrument de paiement d'un autre État partie un traitement moins favorable que celui qu'il accorde aux systèmes de paiement et de règlement numérique ou aux instruments de paiement similaires des autres États parties ou des tiers.

3. Nonobstant les alinéas 1 et 2 du présent article, deux ou plusieurs États parties peuvent maintenir ou conclure des accords ou arrangements préférentiels pour faciliter les paiements numériques transfrontaliers conformément aux objectifs de la présente Annexe.

4. Les États parties à des accords ou arrangements préférentiels visés à l'alinéa 3 du présent article donnent aux autres États parties intéressées la possibilité de négocier les préférences qui y sont accordées sur une base réciproque.

Article 9

Interopérabilité

Les États parties favorisent l'interopérabilité transfrontalière entre les systèmes de paiement et de règlement numériques existants et nouveaux, les cas d'utilisation, les instruments, et les canaux afin de renforcer l'utilisation et l'adoption des paiements numériques, notamment par les moyens suivants :

a. l'adoption de normes internationales de messagerie pour l'échange de données électroniques entre les institutions financières et les fournisseurs de services de paiement numérique ;
b. la facilitation de l'utilisation d'interfaces de programmation d'applications et de plateformes ouvertes, en élaborant des lignes directrices en matière de banque et de finance ouvertes ;
c. l'élimination des obstacles réglementaires et techniques à l'interopérabilité des systèmes de paiement et de règlement numériques ; et

d. la collaboration avec les fournisseurs de services de paiement numérique, les régulateurs, les agrégateurs de paiements et les associations sectorielles concernées sur les normes communes et les solutions techniques.

Article 10

Reconnaissance mutuelle

1. Un État partie reconnaît les instruments de paiement ou les systèmes de paiement et de règlement numériques reconnus et utilisés dans un autre État partie.

2. La reconnaissance visée à l'alinéa 1 du présent article est obtenue conformément aux lois et règlements nationales par voie d'harmonisation ou sur la base d'un accord ou d'un arrangement entre les États parties concernés ou peut être accordée unilatéralement.

3. Lorsqu'un État partie accorde la reconnaissance de manière unilatérale, il donne la possibilité à tout autre État partie de démontrer que ses systèmes de paiement numérique et de paiement devraient être reconnus.

4. Lorsque la reconnaissance est fondée sur un accord ou un arrangement, les autres États parties intéressés se voient accorder une possibilité adéquate de négocier leur adhésion audit accord ou arrangement.

5. Un État partie n'accorde pas la reconnaissance d'instruments de paiement ou de systèmes de paiement et de règlement numériques d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable entre les États parties ou une restriction déguisée aux paiements numériques.

Article 11

Authentification

Les États parties adoptent ou maintiennent des mesures qui permettent l'authentification des paiements numériques transfrontaliers en recourant, entre autres, à l'authentification par certificat, à l'authentification par jeton, à l'authentification biométrique, à la connaissance du client par voie électronique, à l'authentification multifactorielle, à l'identité numérique, à la reconnaissance faciale ou à la signature électronique.

Article 12

Paiements et transferts numériques transfrontaliers

1. Un État partie n'applique pas de restrictions aux transferts transfrontaliers qui sont nécessaires à la conduite du commerce numérique par une personne d'un État partie.

2. Nonobstant l'alinéa 1 du présent article, un État partie peut adopter ou maintenir des restrictions sur les paiements et transferts numériques transfrontaliers liés à la conduite du commerce numérique par une personne d'un État partie :

a. en cas de déficit grave de la balance des paiements ou de difficultés financières extérieures, ou en cas de menace d'un tel déficit ou de telles difficultés ;
b. en cas de blanchiment d'argent, de financement du terrorisme et de prolifération ; ou

c. dans des circonstances exceptionnelles, lorsque les mouvements de capitaux causent ou menacent de causer de graves difficultés économiques ou financières dans l'État partie concerné.

3. Les restrictions visées à l'alinéa 2 du présent article consistent à ce qui suit :

a. ne pas faire de discrimination entre les États parties, les paiements numériques ou les institutions financières ;
b. être conformes aux normes internationales applicables ;
c. éviter de porter inutilement atteinte aux intérêts commerciaux légitimes des ressortissants d'un État partie et des autres États parties ;
d. ne pas excéder celles qui sont nécessaires pour faire face aux circonstances décrites à l'alinéa 2 du présent article ; et
e. être temporaire et progressivement supprimé à mesure que la situation visée à l'alinéa 2 du présent article s'améliore.

4. L'État partie qui adopte ou maintient les restrictions visées dans le présent article ou toute modification de celles-ci en informe rapidement les autres États parties par l'intermédiaire du Secrétariat.

5. Le présent article est sans préjudice des articles 13 et 14 du Protocole sur le commerce des services, et des articles 22 et 23 du Protocole sur les investissements.

Article 13

Taxes et redevances

1. Les États parties adoptent et maintiennent des dispositions législatives ou réglementaires qui imposent aux prestataires de services de paiement numérique de publier ou de mettre à la disposition du public leurs frais respectifs prélevés, directement ou indirectement, sur les paiements numériques afin de promouvoir la transparence et la prévisibilité des frais prélevés sur les paiements numériques transfrontaliers.

2. Les États parties coopèrent pour réduire les coûts de transaction, y compris les frais ou charges prélevés, directement ou indirectement, sur les paiements numériques transfrontaliers, et font en sorte que ces frais soient proportionnels au service rendu.

3. Les États parties coopèrent pour réduire les coûts de mise en conformité avec la réglementation, y compris, mais sans s'y limiter, les frais de licence, les coûts de traitement de la technologie et de l'infrastructure, les exigences du système de détection des fraudes, les coûts juridiques, d'audit et d'établissement de rapports, ainsi que les pénalités et les amendes.

Article 14

Infrastructure de paiement numérique

1. Les États parties coopèrent pour faciliter l'intégration des infrastructures de paiement numérique existantes et futures afin de faciliter les paiements numériques transfrontaliers en :

a. adoptant les normes ou lignes directrices pertinentes en matière d'interopérabilité des systèmes de paiement et de règlement numériques adoptées aux niveaux international, continental et régional ;

b. encourageant leurs banques centrales à faciliter l'interopérabilité des systèmes numériques de paiement et de règlement nationaux, régionaux et continentaux qui traitent à la fois les paiements de détail en temps réel (RTRP) et les règlements bruts en temps réel (RTGS) ; et
c. encourageant les communautés économiques régionales (CER) et les accords commerciaux régionaux à promouvoir l'interopérabilité des RTRP afin de mettre en place un système de paiement et de règlement numérique intégré et interopérable à l'échelle du continent.

2. Les États parties collaborent, si nécessaire, avec toutes les parties prenantes, y compris les CER, les banques centrales, les prestataires de services de paiement, les régulateurs et les organismes de normalisation, pour développer des infrastructures de paiement numérique.

Article 15

Transparence et notification

1. Chaque État partie s'engage dans les meilleurs délais à :

a. publier ou mettre à la disposition du public, y compris par des moyens électroniques, ses lois, règlements, politiques, procédures et décisions administratives d'application générale qui affectent les paiements numériques ou s'y rapportent ; et
b. notifier aux autres États parties, par l'intermédiaire du Secrétariat, l'introduction de toute nouvelle loi ou réglementation ou de tout amendement à des lois et réglementations en vigueur, ou de toute mesure affectant les paiements numériques.

2. Aucune disposition du présent article ne peut être interprétée comme obligeant un État partie à divulguer ou à autoriser l'accès à des informations et données confidentielles dont la divulgation ferait obstacle à l'application des lois ou porterait préjudice aux intérêts commerciaux et stratégiques légitimes d'entreprises ou d'institutions particulières, qu'elles soient publiques ou privées, ou serait de toute autre manière contraire à ses intérêts publics ou essentiels en matière de sécurité.

QUATRIÈME PARTIE

PAIEMENTS NUMÉRIQUES TRANSFRONTALIERS SÛRS ET SÉCURISÉS

Article 16

Cybersécurité

1. En vertu l'article 25 du Protocole, les États parties adoptent ou maintiennent des mesures pour lutter contre la cybercriminalité et les cybermenaces dans le domaine des paiements numériques en tenant compte des meilleures pratiques et normes internationales pertinentes.

2. Les États parties adoptent des dispositions législatives et réglementaires qui imposent aux fournisseurs de services de paiement numérique des obligations de détection et de réaction précoces et de protection contre, entre autres, la cybercriminalité et les cybermenaces.

Article 17

Lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération

1. Chaque État partie adopte ou maintienne des dispositions législatives et réglementaires pour lutter contre le blanchiment de capitaux, le financement du terrorisme et la prolifération des paiements numériques, en tenant compte des meilleures pratiques et normes internationales pertinentes.

2. Les États parties adoptent et maintiennent des dispositions législatives et réglementaires qui imposent aux fournisseurs de services de paiement numérique des obligations en matière de lutte contre le blanchiment d'argent, le financement du terrorisme et la prolifération des paiements numériques.

Article 18

Transfert et protection des données à caractère personnel

1. En vertu de l'article 20 du Protocole, les États parties autorisent le transfert transfrontalier des données de paiement nécessaires pour faciliter les paiements numériques soumis à une surveillance réglementaire appropriée.

2. Nonobstant l'alinéa 1 du présent article, les États parties peuvent restreindre le transfert de données, y compris de données à caractère personnel par des moyens électroniques, afin de protéger les données à caractère personnel, la vie privée et la confidentialité des dossiers et des comptes individuels, y compris, conformément à leurs lois et règlements. Toutefois, de telles restrictions ne doivent pas être utilisées comme un moyen d'éviter les engagements ou les obligations des États parties en vertu de la présente Annexe ou du Protocole.

3. Les dispositions des articles 20 et 21 du Protocole et des dispositions des articles 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 et 21de l'Annexe sur les transferts transfrontaliers de données du Protocole s'appliquent *mutatis mutandis* à la présente Annexe.

Article 19

Pratiques trompeuses et frauduleuses

1. Chaque État partie adopte ou maintient des dispositions législatives et réglementaires pour prévenir les pratiques trompeuses et frauduleuses ou pour faire face aux effets d'un défaut de paiement numérique, en tenant compte des meilleures pratiques et normes internationales pertinentes.

2. Les États parties s'engagent à :

   a. adopter ou maintenir des dispositions législatives et réglementaires qui imposent aux fournisseurs de services de paiement numérique des obligations de protection contre les pratiques trompeuses et frauduleuses dans le domaine des paiements numériques ; et
   b. faciliter l'adoption et l'utilisation de technologies émergentes et avancées pour prévenir les pratiques trompeuses et frauduleuses dans le domaine des paiements numériques, sous réserve des dispositions de l'Annexe sur les technologies émergentes et avancées du Protocole.

Article 20

Protection des consommateurs

Les États parties s'engagent à:

a. faire en sorte que les consommateurs engagés dans le commerce numérique aient facilement accès à des informations claires, complètes et facilement accessibles sur les frais et charges, les taux de change et les mécanismes de règlement des différends pour les paiements numériques transfrontaliers;
b. mettre en place des mécanismes efficaces pour résoudre les litiges liés aux paiements numériques transfrontaliers; et
c. coopérer pour traiter les plaintes ou préoccupations des consommateurs relatives aux paiements numériques transfrontaliers.

Article 21

Réponse aux urgences en matière de paiements numériques transfrontaliers

1. Les États parties s'engagent à:

a. mettre en place ou désignent des équipes nationales ou sectorielles d'intervention d'urgence chargées d'appliquer les dispositions visées aux articles 16, 17, 19 et 20 de la présente Annexe; et
b. par l'intermédiaire de leurs équipes nationales d'intervention d'urgence, cooperer et collaborer pour faire face aux incidents visés aux articles 16, 17, 19 et 20 de la présent Annexe.

2. Les États parties peuvent charger les équipes nationales ou sectorielles d'intervention d'urgence d'établir un registre ou une base de données dans leurs juridictions respectives pour la collecte, le regroupement et l'analyse des incidents couverts par les articles 16, 17, 19 et 20 de la présente Annexe.

Article 22

Coopération

1. Les États parties s'engagent à :
   a. coopérer par l'échange de renseignements, de connaissances et d'expertise, la recherche et le développement, les activités de formation, l'apprentissage en équipe, l'assistance technique, la collaboration entre les secteurs public et privé, le renforcement des capacités et le partage d'expériences et de bonnes pratiques en matière de paiements numériques transfrontaliers ; et
   b. collaborer, si nécessaire, avec les organismes régionaux, continentaux et internationaux compétents pour la mise en œuvre de la présente Annexe.

2. Les États parties peuvent créer un forum continental regroupant les banques centrales, les décideurs politiques, les entreprises de technologie financière, les systèmes de paiement et de règlement continentaux et régionaux, les fournisseurs de services financiers mobiles, les banques et les autres parties prenantes concernées, afin de favoriser la coopération et la collaboration en matière de systèmes de paiement et de règlement numérique transfrontaliers.

3. Les Etats parties coopérent étroitement entre eux, dans le respect de leurs systèmes juridiques et administratifs nationaux respectifs, pour combattre ou prévenir les questions visées aux articles 16, 17 et 19 de la présente Annexe notamment:

   a. echange d'informations et de bonnes pratiques;
   b. assistance judiciaire mutuelle;
   c. campagnes de sensibilisation du public; et
   d. formation et renforcement des capacités des autorités répressives et judiciaires, ainsi que d'autres parties prenantes concernées.

Article 23

Harmonisation des règlements en matière de sécurité et de sûreté

1. Les États parties harmonisent leurs lois et règlements ou mesures visés aux articles 16, 17, 18 et 19 de la présente Annexe.
2. Les Etats parties veillent à ce que :

   a. leurs fournisseurs de services de paiement numérique respectent à tout moment les lois et règlements ou mesures applicables ou visés aux articles 16, 17, 18 et 19 de la présente Annexe.
   b. les lois et règlements ou mesures visés aux articles 16, 17, 18 et 19 de la présente Annexe ne soient pas appliqués d'une manière qui constituerait un moyen de discrimination arbitraire ou injustifiable entre les institutions financières, les paiements numériques ou les États parties, ou une restriction déguisée au système de paiements numériques transfrontaliers ou au commerce numérique.

CINQUIÈME PARTIE

DISPOSITIONS FINALES

Article 24

Règlements et lignes directrices

Les États parties peuvent développer r des réglementations ou des lignes directrices continentales sur l'un des aspects de la présente Annexe afin de faciliter sa mise en œuvre et son application effectives.

Article 25

Règlement des différends

Tout différend entre les États parties, né de l'interprétation ou de l'application de toute disposition de la présente Annexe, est réglé conformément au Protocole sur les règles et procédures relatives au règlement des différends.

Article 26

Révision et modification

La présente Annexe fait l'objet d'une révision et de modification conformément aux articles 28 et 29 de l'Accord sur la ZLECAf, respectivement.

Article 27

Textes authentiques

La présente Annexe est établie en six (6) textes originaux en langues anglaise, arabe, espagnole, française, kiswahili et portugaise, qui font tous également foi.

ANNEXE SUR LA TECHNOLOGIE FINANCIÈRE

PREMIÈRE PARTIE

DISPOSITIONS GÉNÉRALES

Article premier

Définitions

Aux fins de la présente annexe, l'on entend par :

a. **« Annexe »,** l'Annexe sur les technologies financières du Protocole ;
b. **« Technologie financière »,** les technologies qui transforment la fourniture de services financiers, en stimulant le développement de nouveaux modèles d'entreprise, d'applications, de processus et de produits. Il est entendu que ces technologies comprennent, sans s'y limiter, les éléments suivants :
   i. des jeunes pousses et des entreprises de taille réduite spécialisées dans l'innovation financière basée sur la technologie ;
   ii. les institutions financières historiques qui utilisent des modèles de plateforme et qui passent à ces modèles ; et
   iii. des entreprises technologiques offrant des services d'agrégation aux fournisseurs de services financiers numériques.

c. **« Personne d'un État partie »,** une personne d'un État partie telle que définie à l'article 1(p) du Protocole.

Article 2

Objectifs

1. Les objectifs de cette Annexe sont :
   a. donner effet à l'alinéa 2 de l'article 35 du Protocole ;
   b. tirer parti de la technologie financière pour promouvoir les paiements numériques transfrontaliers et stimuler le commerce intra-africain ;
   c. encourager la coopération entre les États parties pour favoriser une innovation et une réglementation responsables des technologies financières ;
   d. promouvoir la collaboration entre les États parties, les entreprises de technologie financière et les organismes du secteur, conformément aux lois et réglementations respectives des États parties ; et
   e. établir des règles harmonisées prévisibles et transparentes, ainsi que des principes et des normes communs pour faciliter le fonctionnement harmonieux des entreprises de technologie financière en Afrique.

Article 3

Champ d'application

1. La présente Annexe s'applique à la technologie financière déployée et utilisée dans le commerce numérique par des ressortissants d'un État partie.
2. La présente Annexe ne déroge pas aux droits et obligations des États parties en vertu du Protocole sur le commerce des services et ne les modifie pas. Il est entendu qu'en

cas de conflit ou d'incohérence entre la présente Annexe et le Protocole sur le commerce des services, les dispositions du Protocole sur le commerce des services prévalent dans la mesure du conflit ou de l'incohérence.

DEUXIÈME PARTIE

RÈGLEMENTS ET NORMES

Article 4

Non-discrimination

1. Un État partie n'accorde pas à la technologie financière concédée sous licence ou enregistrée dans d'autres États parties un traitement moins favorable que celui qu'il accorde à une technologie financière similaire sur son territoire.

2. Un État partie n'accorde pas un traitement moins favorable à une technologie financière concédée sous licence ou enregistrée dans un autre État partie qu'à une technologie financière similaire concédée sous licence ou enregistrée dans d'autres États parties ou dans des tiers.

Article 5

Enregistrement et délivrance de permis

1. Les États parties enregistrent les entreprises de technologie financière et les autorisent à fournir ou faciliter des produits et services financiers conformément à leurs lois et réglementations nationales afin de faciliter le commerce intra-africain.

2. Les États parties adoptent ou maintiennent des cadres juridiques et réglementaires qui permettent aux entreprises de technologie financière de fournir des produits et services financiers.

3. Les États parties peuvent, dans leurs cadres juridiques et réglementaires, autoriser les entreprises de technologie financière à fournir des technologies financières directement et de manière indépendante, sans avoir à s'associer à une institution financière.

4. Les États parties, sous réserve de leurs lois et réglementations, encouragent l'octroi de licences aux entreprises de technologie financière pour qu'elles puissent fournir des paiements numériques ou des services financiers dans plusieurs États parties.

5. Les États parties harmonisent leurs lois et réglementations relatives à l'enregistrement et à l'octroi de licences aux entreprises de technologie financière.

Article 6
Interopérabilité

Les États parties favorisent l'interopérabilité transfrontalière entre les technologies financières, les institutions financières, et les autres prestataires de services de paiement numérique afin de faciliter les paiements et les services numériques, notamment, en :

a. adoptant les normes régionales, continentales, et internationales pertinentes ;
b. facilitant l'accès et l'utilisation d'interfaces de programmation d'applications et de plateformes ouvertes ;
c. éliminant les obstacles réglementaires et techniques inutiles à l'interopérabilité des paiements numériques ; et
d. collaborant avec les fournisseurs de paiements numériques, les agrégateurs de paiements, les régulateurs et les associations sectorielles sur les normes communes et les solutions techniques.

Article 7
Finance ouverte

Les États parties adoptent ou maintiennent, selon qu'il convient, des lois et règlements relatifs à la finance ouverte qui :

a. permettent un échange sécurisé et efficace de données sur les services financiers entre les institutions financières et les entreprises de technologie financière agréées par le biais d'interfaces de programmation d'applications ; et
b. permettent aux entreprises de technologie financière de développer des produits et des services financiers innovants qui exploitent les données fournies par les clients et qui favorisent la réalisation d'avantages potentiels, tels qu'une concurrence accrue et une plus grande valeur pour les clients.

Article 8
Bacs à sable réglementaires

1. Les États parties s'efforcent de créer des bacs à sable réglementaires au niveau national afin de faciliter le développement et l'expérimentation d'innovations en matière de technologies financières dans le cadre d'une surveillance réglementaire, tout en protégeant les consommateurs, en gérant les risques et en préservant la stabilité du système financier.

2. Les États parties font en sorte que les bacs à sable réglementaires :

   a. fournissent un environnement contrôlé qui favorise l'innovation et facilite le développement, l'essai et la validation des cas d'utilisation de la technologie financière pendant une période limitée avant leur déploiement et leur utilisation dans le commerce numérique ou leur entrée sur le marché numérique de la ZLECAf ;
   b. b. permettent, le cas échéant, de tester les technologies financières dans des conditions réelles pendant une période limitée, sous réserve du respect des lois et réglementations relatives à la protection des consommateurs, à la stabilité financière, à la protection des données, et à la cybersécurité.

3. Les États parties s'efforcent d'établir des bacs à sable réglementaires aux niveaux continental et régional pour faciliter le développement et l'expérimentation de la technologie financière par les ressortissants des États parties, y compris les entreprises d'origine africaine.

4. Les bacs à sable réglementaires visés au présent article se concentrent sur les innovations en matière de technologie financière dans des domaines comprenant, sans s'y limiter, le paiement numérique, la technologie de la chaîne de blocs et la technologie réglementaire.

Article 9
Concurrence et innovation

Les États parties encouragent la concurrence et l'innovation dans le domaine des technologies financières en :

a. adoptant des politiques et des lois qui encouragent l'innovation responsable et la concurrence loyale entre les entreprises de technologie financière, et entre les entreprises de technologie financière et les institutions financières ;
b. adoptant des normes régionales, continentales et internationales pertinentes pour les technologies financières, en garantissant un environnement réglementaire harmonisé qui soutient l'innovation tout en protégeant les intérêts des consommateurs et la stabilité financière ;
c. promouvant la recherche et le développement dans le domaine des technologies financières ;
d. encourageant leurs entreprises de technologie financière à utiliser les facilités et l'assistance, lorsqu'elles sont disponibles, sur le territoire d'autres États parties, afin d'explorer de nouvelles opportunités commerciales ;
e. favorisant la collaboration, le dialogue, le partenariat et le transfert de technologie entre leurs entreprises de technologie financière ;
f. adoptant des mesures visant à faciliter l'entrée, l'extensibilité et la viabilité des technologies financières, y compris, mais sans s'y limiter, des programmes d'incubation transfrontaliers, des possibilités de financement et des orientations réglementaires ;
g. mettant en place des centres d'innovation, y compris, mais sans s'y limiter, des centres d'innovation qui favorisent la collaboration et le partage des connaissances entre les entreprises de technologie financière, les secteurs concernés, les universités et les régulateurs ; et
promouvant la connaissance des technologies financières et la sensibilisation des micro, petites et moyennes entreprises africaines, des femmes, des jeunes, des populations autochtones, des communautés rurales et locales, des personnes vivant avec un handicap et d'autres groupes sous-représentés, afin d'accroître l'adoption et l'utilisation des technologies financières.

Article 10
Transparence et notification

1. Chaque État partie s'engage rapidement à :

a. publier ou mettre à la disposition du public dans les meilleurs délais, y compris par des moyens électroniques, ses lois, règlements, politiques, procédures et décisions administratives d'application générale concernant les technologies financières ;
b. notifier rapidement aux autres États parties, par l'intermédiaire du Secrétariat, l'introduction de toute nouvelle loi ou réglementation ou de tout amendement à des lois ou réglementations en vigueur, de toutes mesures concernant ou affectant la technologie financière.

2. Aucune disposition du présent article ne peut être interprétée comme obligeant un État partie à divulguer ou à autoriser l'accès à des informations et données confidentielles dont la divulgation ferait obstacle à l'application des lois ou porterait préjudice aux intérêts commerciaux et stratégiques légitimes d'entreprises ou d'institutions particulières, qu'elles soient publiques ou privées, ou serait de toute autre manière contraire à ses intérêts publics ou essentiels en matière de sécurité.

TROISIÈME PARTIE

SÉCURITÉ ET SÛRETÉ

Article 11
Cybersécurité

1. Conformément à l'article 25 du Protocole, les États parties adoptent ou maintiennent des mesures pour lutter contre la cybercriminalité et les cybermenaces dans le domaine des technologies financières, en tenant compte des meilleures pratiques et normes régionales et internationales pertinentes.

2. Les États parties adoptent des dispositions législatives et réglementaires qui imposent aux entreprises de technologie financière l'obligation d'assurer une détection et une réaction précoces à la cybercriminalité et aux cybermenaces, et de s'en protéger.

Article 12
Lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération

1. Chaque État partie adopte ou maintient des dispositions législatives et réglementaires pour lutter contre le blanchiment de capitaux, le financement du terrorisme et la prolifération des technologies financières, en tenant compte des meilleures pratiques et normes internationales pertinentes.

2. Les États parties adoptent ou maintiennent des dispositions législatives et réglementaires qui imposent aux entreprises de technologie financière l'obligation de lutter contre le blanchiment d'argent et le financement du terrorisme, ainsi que contre la prolifération des technologies financières.

Article 13
Transfert et protection des données à caractère personnel

1. Les États parties adoptent des dispositions législatives et réglementaires qui imposent aux entreprises de technologie financière l'obligation de protéger les données à caractère personnel.

2. Les États parties n'adoptent ni ne maintiennent de mesures empêchant les transferts de données, y compris de données à caractère personnel par voie électronique, nécessaires pour fournir ou faciliter des services financiers numériques par une personne d'un État partie.

3. Lorsqu'ils adoptent ou maintiennent les mesures visées à l'alinéa 2 du présent article, les États parties permettent le transfert transfrontalier sécurisé de données financières pour toutes les entreprises de technologie financière faisant l'objet d'une surveillance réglementaire appropriée. Les dispositions des articles 20 et 21 du Protocole et les dispositions des articles 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 et 21 de l'Annexe sur les transferts transfrontaliers de données du Protocole s'appliquent mutatis *mutandis* à la présente Annexe.

4. Nonobstant l'alinéa 2 du présent article, les États parties peuvent restreindre le transfert de données, y compris de données à caractère personnel, par des moyens électroniques afin de protéger les données à caractère personnel, la vie privée et la

confidentialité des dossiers et des comptes individuels, notamment conformément à leurs lois et règlements. Toutefois, de telles restrictions ne doivent pas être utilisées comme moyen d'éviter les engagements ou obligations d'un État partie au titre de la présente Annexe.

Article 14
Pratiques trompeuses et frauduleuses

1. Chaque État partie adopte ou maintienne des dispositions législatives et réglementaires pour prévenir les pratiques trompeuses et frauduleuses ou pour faire face aux effets d'un défaut sur la technologie financière, en tenant compte des meilleures pratiques et normes internationales pertinentes.

2. Les États parties adoptent et maintiennent des dispositions législatives et réglementaires qui imposent aux entreprises de technologie financière l'obligation de se protéger contre les pratiques trompeuses et frauduleuses.

Article 15
Protection des consommateurs

Les États parties s'engagent à :

a. adopter ou maintenir des dispositions législatives et réglementaires sur les technologies financières pour la protection des consommateurs;
b. adopter ou maintenir des dispositions législatives et réglementaires qui imposent aux entreprises de technologie financière l'obligation de protéger les consommateurs ; et
c. coopèrer pour traiter les plaintes ou les préoccupations des consommateurs en matière de technologie financière et leur offrir des voies de recours.

Article 16
Réponse aux urgences en matière de technologie financière

Les dispositions de l'article 21 de l'Aannexe sur les paiements numériques transfrontaliers du Protocole s'appliquent *mutatis mutandis* aux articles 11, 12, 14 et 15 de la présente Annexe.

Article 17
Harmonisation des règlements en matière de sécurité et de sûreté

Les dispositions de l'article 23 de l'Annexe sur les paiements numériques transfrontaliers du Protocole s'appliquent *mutatis mutandis* aux articles 11, 12, 14 et 15 de la présente Annexe.

Article 18
Coopération

1. Les États parties coopèrent par l'échange de renseignements, de connaissances et d'expertise, la recherche et le développement, les activités de formation, l'apprentissage en équipe, l'assistance technique, la collaboration entre les secteurs public et privé, le

renforcement des capacités et le partage d'expériences et de bonnes pratiques en matière de technologies financières.

2. Les États parties peuvent collaborer à la création d'organismes de certification régionaux ou continentaux sur l'utilisation des technologies financières.

3. Les États parties collaborent, si nécessaire, avec les organismes régionaux, continentaux et internationaux compétents pour la mise en œuvre de la présente Annexe ;

4. Les Etats parties coopèrent étroitement entre eux, dans le respect de leurs systèmes juridiques et administratifs nationaux respectifs, pour combattre et prévenir les questions visées aux articles 11, 12 et 14 de la présente annexe, notamment :

   a. l'échange d'informations et de bonnes pratiques ;
   b. l'entraide judiciaire ;
   c. campagnes de sensibilisation du public ; et
   d. formation et renforcement des capacités des autorités répressives et judiciaires, ainsi que d'autres parties prenantes concernées.

QUATRIÈME PARTIE

DISPOSITIONS FINALES

Article 19
Règlements et lignes directrices

Les États parties peuvent développer des réglementations ou des lignes directrices continentales sur l'un des aspects de la présente Annexe afin de faciliter sa mise en œuvre et son application effectives.

Article 20
Règlement des différends

Tout différend entre les États parties, né de l'interprétation ou de l'application de toute disposition de la présente Annexe, est réglé conformément au Protocole sur les règles et procédures relatives au règlement des différends.

Article 21
Révision et modification

La présente Annexe fait l'objet d'une révision et de modification conformément aux articles 28 et 29 de l'Accord sur la ZLECAF, respectivement.

Article 22
Textes authentiques

La présente Annexe est établie en six (6) textes originaux en langues anglaise, arabe, espagnole, française, kiswahili et portugaise, qui font tous également foi.