Entrée en vigueur de la Convention de Malabo

Au-delà de la bonne nouvelle, les défis de sa mise en œuvre et de son actualisation

Boubacar Diallo
Expert en droit du numérique
Carapaces – Stratégies & Conformités
bdiallo@carapaces.net

How to cite this paper:
Diallo, B. (2024). Entrée en vigueur de la convention de Malabo. Au-delà de la bonne nouvelle, les défis de sa mise en œuvre et de son actualisation. *Global Africa*, (5), pp. 40-55. https://doi.org/10.57832/qw4r-cb16

Received: January 31, 2024
Accepted: February 08, 2024
Published: March 20, 2024

Résumé

La Convention de Malabo, officiellement entrée en vigueur en 2023 après sa ratification par la Mauritanie, représente une étape cruciale vers l'harmonisation des cadres légaux en Afrique concernant la cybersécurité et la protection des données personnelles. Cet instrument juridique, adopté par l'Union africaine en 2014, vise à répondre aux défis posés par l'évolution rapide des technologies de l'information et de la communication (TIC) et à promouvoir la coopération régionale dans ces domaines. Malgré son potentiel significatif pour améliorer la sécurité numérique et la gouvernance des données à l'échelle continentale, l'article souligne la nécessité d'une mise à jour continue de la convention pour intégrer des questions émergentes telles que l'intelligence artificielle et le cyberterrorisme. Il appelle également à une mise en œuvre effective et à une coopération accrue entre les pays africains pour assurer une harmonisation législative réussie, tout en tenant compte des standards internationaux.

Mots-clés

Convention de Malabo, cybersécurité, protection des données, économie numérique, harmonisation législative, Union africaine, intelligence artificielle, cyberterrorisme

Introduction

Le 27 juin 2014, à Malabo en Guinée équatoriale, la Conférence des chefs d'État et de gouvernement de l'Union africaine (UA) adoptait la convention sur la cybersécurité et la protection des données personnelles dite « convention de Malabo ». À travers ce cadre juridique, l'UA visait à définir les objectifs et fixer les grandes orientations de la société de l'information en Afrique et à renforcer les législations des États membres et des communautés économiques régionales (CER) en matière de technologies de l'information et de la communication (TIC). Le 9 mai 2023, la Mauritanie déposait son instrument de ratification, le quinzième[1], marquant ainsi l'entrée en vigueur de la convention, conformément à son article 36, trente jours après sa réception par le président de la Commission de l'UA, soit le 8 juin 2023.

La convention traite, notamment, des transactions électroniques, de la protection des données personnelles, de la promotion de la cybersécurité, ainsi que de la lutte contre la cybercriminalité. Avec son entrée en vigueur, l'Afrique dispose de son premier instrument juridique continental ayant pour vocation d'harmoniser les législations sous-régionales, régionales et nationales, tout en tenant compte des engagements internationaux des États membres en matière de cybersécurité et de protection des données personnelles. Le processus d'élaboration a inclus un large éventail de parties prenantes, dont des experts juridiques, des spécialistes en cybersécurité, des représentants gouvernementaux, ainsi que des acteurs de la société civile, dans le but d'intégrer une diversité de perspectives et d'assurer que la convention fût à la fois exhaustive et adaptée aux réalités spécifiques du continent.

La convention établit un cadre juridique minimal commun pour guider les efforts nationaux et continentaux dans le développement des transactions électroniques, la lutte contre la cybercriminalité, la promotion d'une cybersécurité résiliente, ainsi que la protection des droits humains à travers celle des données personnelles. Son entrée en vigueur apparaît alors, incontestablement, comme une avancée considérable dans la mise en place des conditions juridiques et institutionnelles de la confiance nécessaire au développement du numérique au profit des sociétés africaines. Cela est d'autant plus important qu'à ce jour, de nombreux États membres de l'UA ne disposent pas de cadre juridique dans des domaines couverts par la convention de Malabo[2].

Force est toutefois d'admettre que, dans un domaine aussi évolutif que celui des technologies numériques, l'entrée en vigueur de la convention, neuf ans après son adoption, est bien tardive. De nouvelles technologies ont en effet émergé et d'autres, alors naissantes, sont arrivées à maturité (intelligence artificielle – IA, Big Data, blockchain, impression 3D, IoT…), bouleversant de nombreux secteurs de la vie politique, économique, sociale et culturelle, environnementale et juridique. De nouvelles problématiques juridiques qui accompagnent ces innovations ne trouvent pas de réponses adéquates dans la convention. Le cadre stratégique de l'UA en matière de données[3] ainsi que l'évaluation des besoins en IA en Afrique[4] reflètent également cet écart aujourd'hui important entre les questions couvertes par la convention et les besoins réels de prise en charge des problématiques actuelles liées au marché et à la société numériques en Afrique.

1 Après le Sénégal (16 août 2016), l'Île Maurice (14 mars 2018), la Guinée (16 octobre 2018), la Namibie (1er février 2019), le Ghana (3 juin 2019), le Rwanda (21 novembre 2019), le Mozambique (21 janvier 2020), l'Angola (11 mai 2020), le Congo (23 octobre 2020), la Zambie (24 mars 2021), le Togo (19 octobre 2021), le Cap-Vert (5 février 2022), le Niger (16 mars 2022) et la Côte d'Ivoire (3 avril 2023). https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf. Consulté le 8 novembre 2023.

2 À ce jour, selon les données de la Conférence des Nations unies sur le commerce et le développement (Cnuced), seuls 33 pays (61 %) disposent de législations sur les transactions électroniques et sur la protection des données personnelles, et 39 pays (72 %) sur la cybercriminalité : https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide. Consulté le 8 novembre 2023.

3 Voir : https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-FR.pdf. Consulté le 20 novembre 2023.

4 Voir l'évaluation réalisée sous l'égide de l'Unesco : https://unesdoc.unesco.org/ark:/48223/pf0000375321. Consulté le 20 novembre 2023.

Cela est d'autant plus vrai que l'UA a pris de nouvelles initiatives dans le domaine de la transformation numérique de l'Afrique dans le but de faire émerger une société et une économie numériques intégrées et inclusives, améliorant la qualité de vie des citoyens africains[5]. Cette stratégie globale est pilotée par la Commission de l'Union africaine, en collaboration avec la Commission économique des Nations unies pour l'Afrique (CEA), Smart Africa, l'Agence de développement de l'Union africaine (AUDA-NEPAD), l'Union africaine des télécommunications (UAT), la Fondation pour le renforcement des capacités en Afrique (ACBF), l'Union internationale des télécommunications (UIT) et la Banque mondiale (BM). Elle entend s'appuyer sur les initiatives et les cadres existants tels que l'initiative de politique et de réglementation pour l'Afrique numérique (PRIDA), le programme de développement des infrastructures en Afrique (PIDA), la zone de libre-échange continentale africaine (Zlecaf), les institutions financières de l'Union africaine (AUFI), le marché unique du transport aérien africain (MUTAA) et la libre circulation des personnes (LCP) pour favoriser le développement du marché numérique unique africain (DSM), dans le cadre des priorités d'intégration de l'Union africaine. Cette démarche est en droite ligne de la vision stratégique de Smart Africa pour la création d'un marché unique numérique en Afrique.

De plus, le manque d'infrastructures numériques fiables, les disparités de développement numérique entre les pays, et les variations dans la capacité juridique et technique des États ont un impact certain sur l'opérationnalisation de la convention à travers le continent.

Aussi, tout en se félicitant des avancées réelles induites par l'entrée en vigueur de la convention de Malabo pour de nombreux pays africains, il est essentiel d'en faire une lecture actualisée permettant de tenir compte tant des phénomènes nouveaux liés aux évolutions technologiques que des cadres stratégiques, institutionnels et juridiques qui ont enrichi les référentiels qui sous-tendaient l'adoption de la convention. Une telle lecture permet en effet de dégager les axes d'une mise à jour déjà nécessaire et de réfléchir sur les obstacles à sa mise en œuvre effective. Cette ambivalence entre nécessaire mise en œuvre et impérieuse actualisation constitue le fil de l'équilibre à mettre en lumière afin que l'entrée en vigueur de cette convention soit synonyme d'effectivité et permette également à celle-ci de répondre aux besoins actuels d'une Afrique numérique intégrée et inclusive dans un environnement garantissant la sécurité et la confiance dans le numérique.

Il est en effet crucial de réfléchir sur les conditions essentielles de l'effectivité et de la pertinence de la convention de Malabo pour permettre à l'Afrique de réussir sa stratégie de transformation numérique.

À cette fin, tenant compte du contexte actuel du continent et des problématiques liées aux évolutions technologiques, en droite ligne des orientations stratégiques, institutionnelles et juridiques définies, il est important de procéder à une analyse croisée de la convention et des documents stratégiques et juridiques dans le domaine du numérique en Afrique, à l'image de la stratégie de transformation numérique pour l'Afrique (2020-2030), du cadre stratégique de l'UA en matière de données ou de l'évaluation des besoins en IA en Afrique… L'entrée en vigueur de la convention de Malabo, au regard de l'analyse, apparaît comme tantôt bienvenue avec des acquis à consolider (I), tantôt très attendue malgré des insuffisances à combler (II), tantôt tardive, au regard de toutes les nouveautés à intégrer (III). Cette analyse permet de formuler des recommandations stratégiques pour le futur (IV).

Une entrée en vigueur bienvenue et des acquis à consolider

La convention de Malabo s'articule autour de trois axes majeurs : (i) la promotion de l'économie numérique traduite par les normes relatives aux transactions électroniques, (ii) la protection des droits humains à travers des dispositions sur la protection des données personnelles, et (iii) la promotion et la protection des valeurs essentielles d'une société numérique africaine à travers les dispositions sur la cybersécurité et la cybercriminalité. Cet ensemble a pour dessein de fonder la

5 Outre le cadre stratégique de l'UA en matière de données précité, voir le document de stratégie de transformation numérique pour l'Afrique (2020-2030) : https://au.int/sites/default/files/documents/38507-doc-dts_-_french.pdf. Consulté le 20 novembre 2023.

sécurité et la confiance dans le numérique en Afrique. L'entrée en vigueur de la convention permet ainsi de poser les bases en vue, du point de vue de la démarche, d'harmoniser les cadres juridiques régionaux et nationaux (A) et, du point de vue du contenu, de définir les orientations en matière de transactions électroniques (B), fixer les exigences minimales pour la protection des données personnelles (C) et dessiner les contours de la promotion de la cybersécurité et la lutte contre la cybercriminalité (D).

Harmoniser les cadres juridiques régionaux et nationaux

Il convient de rappeler qu'une initiative, « société africaine de l'information » (AISI), a vu le jour dès 1995 à l'occasion du colloque régional africain sur la télématique au service du développement, organisé en avril 1995 à Addis-Abeba[6]. L'intérêt de l'Afrique pour le numérique s'était ainsi matérialisé très tôt à travers cette initiative, qui faisait de l'harmonisation un de ses principes. Cette démarche s'est d'abord manifestée par le lancement de l'AISI à l'occasion de la conférence sur la société de l'information pour le développement de l'Afrique en mai 1996 en Afrique du Sud, avec la présence de quinze pays africains, ensuite, par son adoption par différents organismes africains, notamment, les ministres africains des Télécommunications à travers la conférence régionale africaine sur le développement des télécommunications tenue à Abidjan en 1996, puis par l'adoption d'une déclaration sur l'AISI par le Conseil des ministres de l'Organisation de l'unité africaine (OUA) à l'occasion du sommet de l'OUA tenu à Yaoundé en juillet 1996. L'AISI a par la suite été intégrée dans le programme de travail de la CEA.

La CEA avait en effet initié un important projet d'harmonisation des législations en matière de TIC en coopération avec la Cedeao et l'Uemoa[7]. C'est dans le prolongement de cette dynamique de convergence qu'a été lancé le projet de Convention de l'Union africaine qui devait permettre la mise en place de règles juridiques destinées à asseoir la sécurité et la confiance dans la société de l'information en Afrique. L'Afrique apparaît ainsi comme précurseur dans la réflexion sur l'évolution vers la société de l'information avec l'AISI créée en 1995 alors qu'au plan mondial, il faudra attendre 2003 et la première phase du sommet mondial sur la société de l'information (SMSI) à Genève (Suisse) et 2005 avec la seconde phase à Tunis (Tunisie) pour voir les déclarations de principe et le plan d'action de Genève ainsi que l'engagement et le plan d'action de Tunis pour la société de l'information[8]. L'élaboration de la convention de Malabo s'inscrivait en droite ligne de cette volonté de l'Union africaine d'accompagner la mise en place d'une société africaine de l'information basée sur la sécurité et la confiance[9].

L'objectif de disposer d'un cadre juridique harmonisé prenant en considération les engagements internationaux et régionaux des États membres est ainsi fortement affirmé et rappelé dans le préambule de la convention[10]. À cette fin, trois enjeux majeurs devaient être pris en compte : le respect des droits humains consacrés par le droit international et le droit africain, le développement de l'économie numérique et la protection des valeurs fondamentales de la société africaine de l'information. C'est ce qui explique l'élargissement de la convention de Malabo, au-delà de la seule question de la lutte contre la cybercriminalité, à celle de la protection des données personnelles et à celle des transactions électroniques.

6 Ce colloque a été organisé « par la Commission économique pour l'Afrique (CEA), en association avec l'Union internationale des télécommunications (UIT), l'Organisation des Nations unies pour l'éducation, la science et la culture (Unesco) et le Centre international de recherche pour le développement (CRDI) qui ont conjugué leurs efforts dans le cadre de l'African Networking Initiative (Initiative relative à la mise en place d'un réseau africain) ». Voir CEA, *Mise en œuvre de l'Initiative « Société africaine à l'ère de l'information » : rapport intérimaire* : https://repository.uneca.org/bitstream/handle/10855/3076/Bib-25638.pdf?sequence=1&isAllowed=y. Consulté le 27 novembre 2023.

7 Cette initiative a conduit à la mise en place, notamment, de l'acte additionnel A/SA.1/01/10, du 16 février 2010 relatif à la protection des données à caractère personnel dans l'espace de la Cedeao.

8 https://www.itu.int/net/wsis/index-fr.html.

9 La convention tient compte de : 1) la Déclaration africaine sur la gouvernance d'Internet dite « d'Oliver Tambo » adoptée par la conférence extraordinaire de l'Union africaine des ministres en charge de la Communication et des Technologies de l'information à Johannesburg le 5 novembre 2009 ; 2) la Déclaration sur les technologies de l'information et de la communication en Afrique : défis et perspectives pour le développement ; 3) la Déclaration d'Abidjan adoptée le 22 février 2012 et celle d'Addis-Abeba adoptée le 22 juin 2012 sur l'harmonisation des cyber-législations en Afrique.

10 Le préambule précise en effet que la convention « vise à la fois à définir les objectifs et les grandes orientations de la société de l'information en Afrique et à renforcer les législations actuelles des États membres et des communautés économiques régionales (CER) en matière de technologies de l'information et de la communication ».

Certes aujourd'hui, au moment où la convention de Malabo est entrée en vigueur, 33 États africains (soit 61 %) disposent déjà de législations sur les transactions électroniques et sur les données à caractère personnel et 39 États (soit 72 %) disposent de législations sur la lutte contre la cybercriminalité[11]. Cela signifie toutefois que sur les 54[12] pays africains reconnus par l'ONU, 28 n'ont pas de législations sur les transactions électroniques et sur les données à caractère personnel et 15 n'en disposent pas sur la lutte contre la cybercriminalité[13]. L'entrée en vigueur de la convention de Malabo constitue une bonne nouvelle tant pour les pays disposant déjà de législations que pour ceux qui n'en disposent pas encore. Pour les premiers, la convention représente un socle minimal qui permet au pays de s'assurer que sa législation prend en compte les exigences d'un cadre juridique en harmonie avec l'existant au plan continental. Pour les seconds, ces exigences minimales permettront à leurs futures législations d'intégrer *ab initio* les objectifs fixés par la convention.

L'entrée en vigueur de la Convention emporte, en effet, pour les États membres, une obligation de transposition en droit interne pour disposer d'un niveau homogène de protection nécessaire à la sécurité et la confiance dans le numérique en Afrique. Cela est d'autant plus important qu'elle tient compte des exigences de conformité avec les cadres juridiques mis en place par les CER, à l'image de la Cedeao, l'Uemoa et la Ceeac. Elle est ainsi bienvenue en ce qu'elle participe de la consolidation des acquis en matière d'harmonisation des législations nationales en posant les bases tant pour les transactions électroniques, les données à caractère personnel que la promotion de la cybersécurité et la lutte contre la cybercriminalité.

Définir les orientations en matière de transactions électroniques

Les technologies numériques constituent un levier puissant de transformation des sociétés et des économies. Leur impact transformationnel est sans précédent en termes de vitesse et d'ampleur[14] et constitue, pour cette raison, une réelle opportunité pour l'Afrique. Consciente de ces perspectives positives, l'UA a eu l'ambition de créer un marché numérique unique sécurisé d'ici 2030[15]. Ce qui était vrai au moment de l'adoption de la convention en 2014 l'est encore davantage aujourd'hui en termes d'importance du développement de l'économie numérique pour promouvoir l'émergence des conditions d'une économie africaine plus prospère. L'Afrique constitue en effet un fantastique réservoir d'utilisateurs de plateformes et de services : 453 millions d'Africains (sur 1,2 milliard) sont aujourd'hui connectés. Cette proportion (35 %) va s'accroître très sensiblement puisque le continent comptera 2,5 milliards d'habitants en 2050[16].

Face à de tels défis, la mise en place d'un cadre juridique approprié constitue un enjeu important pour asseoir la sécurité et la confiance nécessaire au développement de l'économie numérique. Les besoins en investissement pour le développement numérique sont en effet très importants et leur réalisation dépend grandement de la capacité des Africains à mettre en place les conditions de réalisation de tels investissements. L'existence d'un cadre légal et réglementaire favorable au développement de l'économie numérique fait partie de ces conditions.

Les dispositions sur le commerce électronique prévoient les obligations de base que doit respecter tout fournisseur de bien ou prestataire de service électroniques[17] tout en consacrant le principe de soumission de la responsabilité contractuelle du fournisseur aux dispositions nationales pertinentes[18]. Elles encadrent également la publicité par voie électronique en consacrant les

11 Selon les données de la Cnuced, voir : https://unctad.org/page/e-transactions-legislation-worldwide. Consulté le 27 novembre 2023.
12 L'ONU reconnaît officiellement 54 pays africains (https://www.un.org/fr/about-us/member-states) tandis que l'UA en reconnaît officiellement 55 (https://au.int/es/node/34858).
13 Cela inclut les pays sur lesquels la Cnuced ne dispose pas de données sur l'existence de telles législations.
14 Une augmentation de 10 % de la pénétration du haut débit mobile dans les économies à faibles revenus entraîne une augmentation de 2 % du PIB. En Afrique subsaharienne, cette tendance est encore plus marquée puisqu'une augmentation de 10 % de la pénétration du haut débit mobile devrait y entraîner une augmentation de 2,5 % du PIB. Cf. UIT, *Economic Contribution of Broadband, Digitization and ICT Regulation: Econometric Modelling for Africa*, 2019, https: www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.BDT_AFR-2019-PDF-E.pdf. Consulté le 27 novembre 2023.
15 Cf. Stratégie de transformation numérique pour l'Afrique (2020-2030), *op. cit*.
16 M. Olivier et S. Ballong, « Gafam : l'Afrique face aux géants du Web », dossier publié le 16 août 2018. Cf. https://www.jeuneafrique.com/mag/614444/societe/gafam-lafrique-face-aux-geants-du-web/. Consulté le 29 janvier 2024.
17 Cf. notamment, art. 2 de la convention qui indique les informations et mentions obligatoires à respecter.
18 Cf. art. 3 de la convention.

engagements des États parties, notamment en matière de prospection. Les contrats du commerce électronique sont également consacrés en précisant les modalités de leur conclusion et en consacrant l'écrit et la preuve électronique. Ce principe trouve ainsi une place importante dans la convention qui renvoie aux États parties pour en fixer les conditions légales. Les dispositions sur la sécurisation des transactions électroniques tirent les conséquences de la signature électronique pour la validité des modes de paiement électronique ainsi que la force probante des actes revêtus d'une signature électronique qualifiée.

De telles dispositions sont essentielles pour créer les conditions d'existence et de développement du commerce électronique, même si le contexte et les enjeux ont beaucoup évolué et rendent nécessaire une évolution des dispositions de la convention. Ce sont toutefois des orientations de base pour les législations des États auxquelles s'ajoutent des exigences minimales pour la protection des données personnelles.

Fixer les exigences minimales pour la protection des données personnelles

L'Union africaine a tenu à rappeler dans la convention son attachement aux engagements internationaux et africains en matière de protection de la dignité humaine et des droits humains qui en découlent. Or dans le numérique, les données personnelles partagées par les usagers constituent une source constante d'inquiétude pour la préservation de la dignité des individus, la confidentialité et, plus largement, la protection de leurs droits. C'est pour cela que la convention a rappelé que la protection des données à caractère personnel ainsi que de la vie privée est un enjeu majeur de la société de l'information, tant pour les pouvoirs publics que pour les autres parties prenantes. Elle considère que cette protection nécessite un équilibre entre l'usage des TIC et la protection de la vie privée des citoyens dans leur vie quotidienne ou professionnelle, tout en garantissant la libre circulation des informations.

En soulignant les engagements des États pour la mise en place d'un cadre juridique de protection des données personnelles, la convention impose, selon le cas, une formalité de déclaration préalable ou d'autorisation. Elle consacre également d'importantes dispositions au cadre institutionnel que chaque État partie doit mettre en place pour la protection de ces données. Les attributions de ces autorités nationales sont précisées de même que leurs pouvoirs. D'un point de vue substantiel, la convention fixe, d'une part, les principes à respecter en matière de traitement des données personnelles et précise le régime spécifique des données sensibles ou de l'interconnexion de fichiers comportant ce type de données et d'autre part, les droits des personnes titulaires des données personnelles traitées et les obligations du responsable de leur traitement.

Les dispositions relatives à la protection des données instaurent ainsi des garde-fous pour assurer que les informations personnelles des citoyens soient manipulées de manière sécurisée et éthique. Par conséquent, elle offre un cadre qui garantit une plus grande sécurité et veille à préserver la vie privée des citoyens dans l'espace numérique. Les dispositions relatives à la cybersécurité et à la lutte contre la cybercriminalité confortent ce dispositif de sécurisation.

Dessiner les contours de la promotion de la cybersécurité et de la lutte contre la cybercriminalité

Lorsque l'on évoque les opportunités qu'offre le numérique, on ne peut taire les risques importants qu'il comprend également. Promouvoir le développement d'un marché numérique sécurisé en Afrique suppose ainsi qu'il existe un cadre juridique de confiance.

Ainsi, l'Union africaine avait compris l'urgence de la mise en place, à travers la convention, d'un dispositif permettant de faire face aux dangers et risques nés de l'utilisation de l'informatique et des fichiers sur les individus dans le souci de respecter la vie privée et les libertés, tout en favorisant la promotion et le développement des TIC dans ses pays membres. La promotion de la cybersécurité comme la lutte contre la cybercriminalité tiennent ainsi une place centrale dans la convention.

La mise en place d'une législation harmonisée dans le domaine de la cybersécurité dans les États membres de l'UA passait dès lors par l'adoption de règles juridiques minimales permettant aux États, aux organisations publiques, privées et sociétales, ainsi qu'aux individus en leur sein, d'avoir conscience des risques et de se prémunir contre les atteintes multiples aux droits des usagers, aux infrastructures et systèmes d'information, aux données, etc. qu'entraîne le numérique. Et lorsque de telles atteintes mettent en cause les valeurs jugées essentielles de la société et du marché, une protection pénale du système de valeurs de la société de l'information s'impose comme une nécessité à travers les dispositions consacrées à la lutte contre la cybercriminalité.

Tenant compte des engagements des États aux plans sous-régional, régional et international, la convention fixe les grandes orientations de la stratégie de répression de la cybercriminalité afin de protéger les réseaux informatiques et la société de l'information de la menace cybercriminelle.

À cette fin, du point de vue du droit pénal substantiel, la convention avait pour but de moderniser les instruments de répression de la cybercriminalité. D'une part, de nouvelles incriminations spécifiques aux TIC ont été consacrées afin d'appréhender les nouveaux phénomènes criminels induits par ces technologies. D'autre part, des incriminations existantes ont été adaptées, tout comme les sanctions et le régime de responsabilité pénale en vigueur dans les États membres afin de les mettre en adéquation avec les spécificités de l'environnement des technologies de l'information et de la communication. En dehors de certaines atteintes aux biens, l'innovation la plus importante à ce niveau concernait la responsabilité pénale des personnes morales que la convention impose aux États parties de rendre effective en droit interne.

Du point de vue du droit pénal procédural, la même démarche a été adoptée consistant, d'une part, à instituer de nouvelles procédures spécifiques à la cybercriminalité dans la mesure où les procédures existantes ne permettent pas de traiter des phénomènes liés aux technologies en cause et d'autre part, à aménager la procédure existante pour en adapter la mise en œuvre aux technologies de l'information et de la communication.

L'objectif de ce dispositif de promotion de la cybersécurité et de lutte contre la cybercriminalité était la sécurisation du cyberespace en Afrique comme prérequis essentiel pour le développement économique numérique. Avec l'ambition d'instaurer un environnement numérique sûr et régulé, la convention de Malabo visait également à encourager les investissements nécessaires au développement dans le secteur numérique en favorisant l'innovation technologique. L'entrée en vigueur de la convention y participera sans doute et, pour cette raison, était fortement attendue malgré des insuffisances à combler.

Une entrée en vigueur attendue mais des insuffisances à combler

L'entrée en vigueur de la convention de Malabo était attendue pour offrir un cadre juridique harmonisé sur la protection des données personnelles, les transactions électroniques, la promotion de la cybersécurité et la lutte contre la cybercriminalité. Toutefois, dès son adoption, sont apparues des insuffisances dont certaines peuvent être considérées comme consubstantielles au processus d'adoption, ainsi qu'à la nature juridique de la convention. La pertinence discutable de certaines dispositions (A), sa force contraignante limitée (B), l'absence de cadre institutionnel de mise en œuvre (C), de même que l'absence de mécanismes permanents de mise à jour (D) de la convention sont autant d'insuffisances à combler.

Pertinence discutable de certaines stipulations

La « mal nommée » convention de l'Union africaine sur la cybersécurité et la protection des données personnelles traite également des transactions électroniques et de la cybercriminalité. Cet intitulé est très réducteur car il ne rend pas compte de l'ensemble des problématiques juridiques traitées relatives au triple enjeu précité. Certains intitulés du projet initial étaient plus pertinents et englobants car ils mettaient l'accent, de manière positive, sur le besoin de confiance ou de sécurité

 https://doi.org/10.57832/qw4r-cb16

dans la société de l'information que la convention devait permettre de combler[19]. Mettre l'accent sur les besoins de confiance et de sécurité dans le numérique permet, non seulement d'englober l'ensemble des problématiques traitées dans la convention, mais également de présenter celle-ci comme un moyen de combler ces besoins essentiels pour les États, les organisations publiques, privées et sociétales, mais aussi les individus et l'ensemble des parties prenantes dans une société et un marché numériques. Mais au-delà de sa dénomination, d'autres dispositions de la convention ont une pertinence discutable.

Certaines consacrées à la protection des données personnelles peuvent notamment être remises en question quant à leur pertinence. Elles prévoient, sauf cas exceptionnels prévus, des formalités préalables (article 10) de déclaration ou d'autorisation, selon le cas, qui peuvent paraître lourdes à mettre en œuvre en raison du nombre de systèmes de traitement mis en œuvre dans une société de plus en plus numérique. Un système qui responsabilise davantage les chargés de traitement et organise un contrôle *a posteriori* plus efficace pourrait être plus adapté. Elles prévoient également que l'autorité de protection des données personnelles doit être une autorité indépendante (article 11), mais sans définir les critères de cette indépendance qui est pourtant centrale dans le succès du dispositif de protection.

D'autres dispositions consacrées aux transactions électroniques peuvent également soulever des interrogations sur leur pertinence, notamment leur capacité à encadrer les transactions administratives et les transactions financières de plus en plus développées en Afrique, aussi bien que les transactions commerciales qui semblent être les seules réellement prises en compte. Certes, d'autres autorités, notamment régionales ou nationales (banques centrales régionales ou nationales ou commissions bancaires et autorités de marchés financiers) ont compétence pour réguler ces transactions, mais la convention peut offrir un cadre général harmonisé à l'échelle africaine, surtout dans la perspective d'un marché numérique africain.

Enfin, les dispositions prévues en matière de lutte contre la cybercriminalité ne comportent pas de règles de droit international privé permettant de traiter des conflits de lois et de compétence juridictionnelle qui peuvent se poser en matière de cybercriminalité.

Ces insuffisances viennent s'ajouter à une force contraignante limitée de la convention de Malabo malgré son entrée en vigueur.

Force contraignante limitée de la convention

L'entrée en vigueur de la convention de Malabo permet de la rendre applicable à l'ensemble des États membres. Son applicabilité ne signifie toutefois pas possibilité pour les justiciables des États parties de se prévaloir directement de ses dispositions et de les opposer aux autorités nationales notamment. Il n'existe pas d'effet direct de la convention de Malabo. Elle n'a pas davantage d'effet immédiat, car elle nécessite que chaque État partie prenne les mesures légales et réglementaires en vue de la transposition de ses dispositions en droit interne.

Malgré son entrée en vigueur, la force contraignante de la convention reste ainsi très limitée au regard du besoin d'intervention des États parties pour que les dispositions soient applicables en droit interne. Les moyens de « convaincre » les États membres de prendre de telles dispositions sont également très limités en l'absence de sanctions effectives. Or comme indiqué précédemment, de nombreux pays ne disposent pas encore de législations dans les domaines couverts par la convention, et les justiciables de ces pays sont ainsi exposés face aux phénomènes de la société et du marché numériques. Ces dispositions leur offriraient pourtant un cadre juridique minimal pour l'économie, la protection des données personnelles, la cybersécurité et la lutte contre la cybercriminalité.

19 Un « projet de convention de l'Union africaine sur la mise en place d'un cadre juridique de confiance pour la cybersécurité en Afrique » est encore disponible en ligne. La version de la convention publiée sur le site de la commission de protection des données personnelles (CDP) du Sénégal est bien intitulée « Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel », sur la page de garde, mais dans l'article 1 consacré aux définitions apparaît pour « (La présente) convention », « Convention de l'Union africaine sur la confiance et la sécurité dans le cyberespace ». Sans doute la publication de la CDP sera-t-elle vite supprimée, mais il faut souhaiter que cette archive sera sauvegardée non seulement pour la mémoire, mais également pour la meilleure pertinence de l'intitulé qu'elle propose. Voir notamment le projet : https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/draft%20convention%20cybersecurity%20french%2019%20sept%202011.pdf. Consulté le 28 novembre 2023.

L'absence de cadre institutionnel de mise en œuvre de la convention à l'échelle de l'UA ne permet pas de combler les insuffisances liées à la force contraignante limitée.

Absence de cadre institutionnel effectif de mise en œuvre et de suivi

L'adoption de la convention de Malabo n'a pas été accompagnée de la mise en place d'un cadre institutionnel effectif pour sa mise en œuvre. Certes, l'article 32 fixe des mesures de suivi à prendre au niveau de l'UA, mais l'ineffectivité de telles mesures n'a pas permis de prendre convenablement en charge certaines problématiques.

La mise en place effective d'un cadre institutionnel de mise en œuvre avec une démarche articulée aux CER avait d'ailleurs été proposée et envisagée par l'équipe d'experts ayant travaillé à la conception et la rédaction de la convention[20]. Basée sur des textes régionaux préexistants, notamment ceux de la Cedeao[21], la stratégie de ratification proposée reposait sur un dispositif institutionnel de suivi des ratifications articulé à cette CER dont les États membres disposaient déjà dans une large mesure de textes juridiques internes au moins équivalents à une transposition des dispositions de la convention. Nul doute qu'une telle démarche institutionnelle aurait permis d'abréger le délai de l'entrée en vigueur de la convention.

Les personnes-ressources à la base de la conception et l'adoption de la convention auraient pu être mises à contribution à travers un tel cadre institutionnel. Elles auraient également pu être renforcées par de nouvelles compétences et expertises africaines. Cela aurait également sans doute permis d'offrir aux États membres une assistance en termes d'expertise et de compétence dans un domaine aussi technique et à si forts enjeux dans le but d'accélérer les processus de ratification et de transposition en droit interne.

Absence de mécanismes permanents de mise à jour

La vitesse et l'ampleur de l'expansion des technologies nouvelles se sont exponentiellement accrues. Lancé en 1878, le téléphone a mis soixante-quinze ans à atteindre 100 millions d'utilisateurs. Ce temps a été réduit à seize ans pour le téléphone portable lancé en 1979, puis à quatre ans et six mois pour Facebook après son lancement en 2004, puis à trois ans et quatre mois pour WhatsApp, lancé en 2009[22], pour atteindre soixante jours pour ChatGPT[23], lancé en 2022, ce record ayant ensuite été vite battu par Threads[24] en cinq jours après son lancement en juillet 2023.

Dans un monde numérique où la technologie évolue à un rythme fulgurant, la convention doit être souple et adaptable aux nouvelles réalités et défis du cyberespace. Cela signifie que le texte et les dispositions devraient être révisables et modifiables pour s'adapter, notamment, aux nouveaux défis juridiques liés aux technologies émergentes. L'intégration d'un mécanisme qui permet une révision et une mise à jour périodiques est vitale pour garantir qu'elle reste pertinente et efficace face aux défis changeants et aux dynamiques de la société et du marché numériques.

Certes, la convention prévoit un mécanisme d'amendement ou de révision (article 37) ainsi que des mécanismes de suivi déjà évoqués (article 32), mais ces mécanismes ne semblent pas adaptés pour une mise à jour régulière en vue de l'adapter à l'évolution du numérique. Tels qu'envisagés, les amendements ou révisions sont soumis par tout État partie, ce qui signifie que l'initiative appartient aux États parties.

L'existence d'un cadre institutionnel de mise en œuvre évoqué plus haut aurait pu faciliter la mise en place de mécanismes de mise à jour régulière. Celle-ci pourrait être confiée à l'organe de suivi et de mise en œuvre composé d'experts reconnus dans le domaine ainsi que des parties prenantes qui seraient chargés de faire de la veille technologique et juridique afin de proposer, sur une base

20 Voir A. Cissé, « la Convention de Malabo, l'impérieuse actualisation ! », communication prononcée à l'occasion de la session « Samm sunuy données » du Laspad.
21 Voir l'acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel dans l'espace de la Cedeao, *op. cit*.
22 https://www.vingthuitzerotrois.fr/reflexion-business/graphique-du-temps-pour-acceder-a-100-millions-dutilisateurs-15990/.
23 https://www.theguardian.com/technology/2023/feb/02/chatgpt-100-million-users-open-ai-fastest-growing-app.
24 https://www.forbes.com/sites/siladityaray/2023/07/10/with-100-million-users-in-five-days-threads-is-the-fastest-growing-app-in-history/?sh=17a6890f49ab.

périodique définie dans la convention (une périodicité au moins annuelle), les mises à jour destinées à encadrer les phénomènes induits par les évolutions technologiques importantes. Le processus d'amendement pourrait alors être fixé dans la convention, ce qui aurait sans doute évité une impérieuse actualisation dès sa mise en application.

Une entrée en vigueur tardive et des nouveautés à intégrer

La vitesse et l'ampleur des évolutions technologiques et des phénomènes qu'elles induisent rendent obsolètes beaucoup de dispositions juridiques sans cesse dépassées par la réalité du numérique. Depuis l'adoption de la convention, nombre de phénomènes nouveaux ont vu le jour. Son entrée en vigueur tardive rend impérieuse son actualisation au regard, notamment, du cyberterrorisme et la sécurité nationale (A), de l'éthique et la gouvernance de l'IA et des technologies émergentes (B), de l'encadrement des marchés et services numériques en Afrique (C), ou encore de la problématique des droits numériques et de l'inclusion en Afrique (D).

Cyberterrorisme et sécurité nationale

La convention de Malabo entendait mettre en place un cadre juridique de promotion de la cybersécurité et de la lutte contre la cybercriminalité. À l'heure de son entrée en vigueur, de nouveaux risques et menaces ont vu le jour ou pris une nouvelle ampleur. Des attaques cybercriminelles visent de plus en plus des infrastructures critiques et des intérêts stratégiques nationaux mettant en cause la sécurité nationale. De nouvelles formes de guerres numériques existent et font peser des risques importants pour la défense nationale.

Ainsi, bien que la convention ait mis un point d'honneur à aborder divers aspects de la cybersécurité et de la cybercriminalité, l'implication du cyberterrorisme, particulièrement en matière de sécurité nationale, requiert une attention plus approfondie. Les attaques cyberterroristes, qui visent des infrastructures critiques, peuvent avoir des répercussions désastreuses non seulement sur l'économie, mais aussi sur la stabilité socio-politique des États parties. Une analyse détaillée des menaces actuelles et potentielles, combinée à l'élaboration de stratégies robustes et adaptées pour contrecarrer ces menaces, est indispensable.

Dans cette optique, la convention pourrait intégrer de nouvelles dispositions spécifiques en vue de cibler le cyberterrorisme, consacrer de nouvelles infractions ou adapter des infractions existantes à ce type de menaces liées aux infrastructures critiques, logiciels malveillants, désinformation ou exploitation des réseaux sociaux pour le recrutement, l'organisation ou la perpétration d'actes terroristes. Elle pourrait également donner des orientations sur le cadre institutionnel et les mécanismes à mettre en place, ainsi que les mesures de protection des infrastructures critiques, de renforcement des capacités, de collaboration avec le secteur privé et la société civile, ou encore la mise en place de cadres juridiques nationaux en matière de cyberdéfense.

Il serait également judicieux d'intégrer des mécanismes de coopération sous-régionale, régionale et internationale renforcée pour un échange efficace d'informations et de pratiques en matière de lutte contre le cyberterrorisme.

L'ensemble de ces mesures devra être conçu et mis en œuvre de manière à respecter les droits humains et les libertés civiles, tout en assurant une sécurité efficace contre les menaces du cyberterrorisme.

Éthique et gouvernance de l'IA et des technologies émergentes

La montée de l'intelligence artificielle (IA) et d'autres technologies émergentes présente des défis éthiques et de gouvernance considérables qui semblent échapper au cadre de la convention en vigueur. Le recours à l'IA dans divers secteurs (sécurité, santé, éducation, migration, etc.) soulève de multiples questions liées à des principes essentiels pour une IA éthique et responsable, qui méritent une exploration minutieuse. Une mise à jour de la convention pourrait permettre l'intégration de

lignes directrices éthiques et de cadres de gouvernance pour assurer un développement et une utilisation responsables de l'IA, garantissant ainsi que ces technologies bénéficient à tous les citoyens de manière équitable.

En vue de tenir compte de la complexité de la gouvernance de l'IA et des technologies émergentes qui nécessite une approche multidimensionnelle, les orientations d'une mise à jour de la convention devraient comprendre des principes et des règles essentiels qui gouverneraient leur conception et leur mise en œuvre, notamment :

- **transparence et responsabilité** pour que les processus et les décisions de l'IA soient transparents et que les développeurs et les utilisateurs de ces technologies soient tenus responsables de leurs actions et des résultats produits ;
- **équité et non-discrimination** pour que l'IA soit conçue et utilisée de manière à éviter les biais et discriminations, qu'ils soient raciaux, de genre, d'âge ou autres, ce qui nécessite des efforts constants pour s'assurer que les systèmes d'IA traitent tous les utilisateurs de manière équitable ;
- **fiabilité et sécurité** des systèmes d'IA pour leur permettre de fonctionner comme prévu et être protégés contre les manipulations et les abus ;
- **interopérabilité** pour que les systèmes d'IA soient capables de fonctionner avec d'autres systèmes et technologies, tout en respectant les normes et les protocoles établis ;
- **innovation responsable** pour encourager l'innovation tout en veillant à ce que les développements technologiques soient éthiques et alignés sur les valeurs humaines et le bien-être sociétal ;
- **respect de la vie privée et des données** comme priorités majeures, ce qui implique des mesures de sécurité robustes et le respect des législations sur la protection des données ;
- **inclusion et accessibilité** de l'IA à tous, indépendamment de la capacité économique, de la situation géographique, du handicap, etc., ce qui induit la conception de technologies inclusives et la garantie d'un accès équitable ;
- **bien-être humain et impact social** pour que l'IA soit développée et utilisée de manière à promouvoir le bien-être humain, en considérant les impacts sociaux, économiques et culturels ;
- **dialogue et participation des parties prenantes** car la gouvernance de l'IA devrait inclure un dialogue ouvert avec diverses parties prenantes, y compris la société civile, le public, les experts en éthique, l'industrie, et les gouvernements ;
- **coopération sous-régionale, régionale et internationale** qui est essentielle puisque, compte tenu de la nature transfrontalière de l'IA et des technologies émergentes, elle est essentielle pour développer des normes et des règles harmonisées ;
- **formation et sensibilisation** car il est important d'éduquer et de former les acteurs publics, privés et sociétaux, les développeurs, les utilisateurs et le grand public sur les enjeux, les possibilités et les risques associés à l'IA ;
- **adaptabilité et flexibilité** puisque les réglementations et politiques en matière d'IA doivent être suffisamment flexibles pour s'adapter à l'évolution rapide des technologies ;
- **respect de l'environnement** pour que les technologies émergentes soient développées et utilisées d'une manière qui soit durable et respectueuse de l'environnement.

De tels principes et règles pourraient constituer des orientations qui seraient également adaptées en fonction des contextes spécifiques et des évolutions technologiques. Ils seraient un cadre de base pour une gouvernance éthique et responsable de l'IA et des technologies émergentes.

Encadrement des marchés et services numériques africains

L'ambition de l'UA de faire émerger une économie numérique intégrée et inclusive en Afrique suppose la création d'un marché numérique continental dynamique et prospère. La mise en place de la Zlecaf constitue, de ce point de vue, une réelle opportunité car elle « créerait un marché continental de 1,3 milliard de personnes avec un PIB combiné de 3 400 milliards de dollars, ce qui en ferait la plus grande zone de libre-échange au monde depuis la création de l'Organisation mondiale du commerce… La Zlecaf devrait stimuler le commerce intra-africain de 52,3 % d'ici 2025, augmenter les revenus de l'Afrique jusqu'à 450 milliards de dollars d'ici 2035, selon le FMI[25], et sortir 30 millions d'Africains de l'extrême pauvreté[26] ». Le marché numérique en particulier, compte tenu des opportunités qu'il offre ainsi que de la vitesse et de l'ampleur de la pénétration des technologies dans tous les domaines, peut permettre de libérer « le potentiel du commerce numérique en Afrique et permettre aux entreprises, en particulier les petites et moyennes entreprises, d'étendre leur portée et de puiser dans de nouveaux marchés[27] ».

Une mise à jour de la convention peut être l'occasion de mettre en place un encadrement adéquat de ce marché numérique africain en cohérence avec l'accélération de la mise en œuvre de la Zlecaf. Son encadrement ainsi que celui des services numériques permettrait d'intégrer une approche plus globalisante du commerce électronique tel qu'envisagé dans la convention en vigueur, en tenant compte des défis associés tels que la fiscalité numérique et une protection approfondie des consommateurs en ligne. Elle permettrait surtout de consacrer des règles et des principes essentiels pour un marché numérique continental africain ouvert, intégré et inclusif.

L'un des piliers d'un tel marché devrait consister dans l'organisation d'une concurrence libre et saine entre ses divers acteurs. À cette fin, les règles et principes consacrés par l'UA à travers la convention devraient permettre d'empêcher les pratiques anticoncurrentielles et assurer un marché numérique ouvert et équitable pour les petites et les grandes entreprises. L'accès équitable au marché devrait être assuré, dans un contexte de marché numérique mondial ultra dominé par des méga-plateformes dont dépendent des milliers de professionnels. Les règles doivent permettre de s'assurer que les grandes plateformes n'abusent pas de leur position dominante pour discriminer certaines entreprises ou consommateurs, ou pour favoriser leurs propres services ou produits. Les entreprises technologiques doivent être transparentes quant à leurs algorithmes, leurs politiques de collecte de données et leurs pratiques commerciales. La responsabilité pour les contenus publiés et les actions menées en ligne est cruciale. Les plateformes numériques doivent être tenues responsables du contenu qu'elles hébergent, avec des réglementations qui équilibrent la liberté d'expression et la lutte contre les discours de haine, la désinformation, et le contenu illégal.

Les règles destinées à l'encadrement d'un marché numérique africain devraient également promouvoir la protection des droits d'auteur et de la propriété intellectuelle pour encourager l'innovation et protéger les créateurs. Elles devraient également encourager les entreprises numériques à prendre en compte leur impact environnemental, notamment en termes de consommation d'énergie et de déchets électroniques.

Une attention particulière devrait également être consacrée, d'une part, à la protection des consommateurs contre les pratiques abusives ou trompeuses tout en encourageant l'innovation et d'autre part, aux travailleurs numériques en vue de protéger leurs droits spécifiques, y compris les travailleurs des plateformes et les travailleurs à distance.

La mise en œuvre de l'ensemble de ces principes et règles nécessite une collaboration étroite avec les différentes institutions intervenant en matière de développement économique à l'échelle africaine (CEA, Zlecaf, AUDA-NEPAD…), celles qui interviennent dans le domaine du numérique (Smart Africa, etc.), avec les institutions internationales, les CER, les gouvernements, les entreprises technologiques, la société civile et les usagers pour créer un environnement numérique équilibré et durable.

25 Fonds monétaire international.

26 Cf. « Zlecaf : Saisir les opportunités pour une Afrique prospère », dans *Afrique Renouveau*, mai 2023, par Mme Nardos Bekele-Thomas, directrice générale de l'AUDA-NEPAD, bras armé de l'UA en matière de développement : https://www.un.org/africarenewal/fr/magazine/mai-2023/zlecaf-saisir-les-opportunités-pour-une-afrique-prospère#:~:text=La%20ZLECAf%20est%20en%20vigueur,%22%20par%20l%27Union%20africaine.

27 *Op. cit*.

Droits numériques et inclusion numérique

Dans le prolongement de la mise en place de dispositions consacrées au marché et services numériques en Afrique, il est important de consacrer une attention particulière à l'inclusion numérique et aux droits numériques. Dans un contexte africain, il est en effet essentiel de s'assurer que tous les groupes de la société ont accès aux technologies numériques et sont capables de les utiliser efficacement, en particulier les personnes les plus vulnérables. L'accès aux services numériques devrait être équitable, sans discrimination basée sur la localisation, les revenus, ou d'autres facteurs.

Divers droits devraient être consacrés et garantis par les dispositions de la convention. Celle-ci affirme déjà son attachement au respect des droits humains et certains aspects déjà pris en compte pourraient être approfondis. Il est impératif de prendre en considération l'accès universel à Internet comme fondamental pour garantir l'inclusion numérique et sociale de tous les citoyens. La convention devrait ainsi promouvoir des stratégies et des politiques qui visent à garantir un accès équitable et abordable à Internet, tout en protégeant les droits numériques des utilisateurs.

De manière spécifique, certains droits particuliers devraient être consacrés, notamment (i) le droit à la portabilité des données en vertu duquel les utilisateurs pourraient transférer facilement leurs données d'une plateforme à une autre pour favoriser la concurrence, (ii) le droit à la réparation qui favoriserait la durabilité des produits numériques, réduirait les déchets électroniques et promouvrait une économie plus durable.

L'éducation et la sensibilisation sont, à ce propos, une dimension importante. Éduquer les consommateurs et les entreprises sur leurs droits et responsabilités est en effet crucial pour un environnement concurrentiel sain au sein du marché numérique en Afrique.

Enfin, il est essentiel de traiter de la question des droits numériques et de l'inclusion numérique aussi bien à l'échelle des États qu'à celle des entreprises et des individus. Il est important que les pays les plus victimes d'exclusion numérique en Afrique reçoivent une attention particulière.

Recommandations stratégiques pour le futur

La convention de Malabo étant en vigueur, il est essentiel de s'assurer que les conditions de sa mise en œuvre soient assurées à travers les mesures d'accompagnement (A) adéquates. L'impérieuse nécessité de sa mise à jour (B) en raison, notamment, des évolutions technologiques importantes ne doit pas faire perdre de vue son utilité pour nombre de pays africains malgré les insuffisances relevées. En tirant les leçons de cette première version, il est possible de mieux préparer son avenir à travers un cadre institutionnel et des mécanismes de mise à jour permanente (C) de la prochaine version, tout en renforçant la coopération et l'harmonisation régionales et internationales (D) en adéquation avec les autres projets et programmes à l'échelle du continent.

Mettre en place des mesures d'accompagnement de l'entrée en vigueur

L'accompagnement de la mise en œuvre de la convention de Malabo requiert la mise en place d'une stratégie claire qui implique la sensibilisation et la communication, l'engagement des parties prenantes ainsi que le renforcement des capacités nationales.

La **sensibilisation** et la **communication** constituent en effet un premier axe stratégique clé de la mise en œuvre de la convention, permettant la dissémination d'une information correcte auprès des cibles pertinentes. Diverses mesures seraient, à ce propos, envisageables. Il est essentiel d'utiliser le numérique par la création d'une page web dédiée à la convention ainsi que des comptes et pages spécifiques sur les principaux réseaux sociaux utilisés sur le continent. Autour de ces instruments numériques peuvent se bâtir des campagnes de sensibilisation et d'information focalisant sur des messages clairs à propos de la convention. Divers outils enrichis de l'IA permettent de rendre ces contenus disponibles sur divers supports (écrit, audio, vidéo, jeux interactifs, etc.) dans différentes langues, dont les langues nationales. D'autres outils (sondages, feedbacks, analyse de données de

participation…) peuvent permettre d'en mesurer l'impact. Des guides, brochures et autres matériels de communication peuvent également être élaborés à destination de certains acteurs clés de la mise en œuvre ou du grand public.

L'**engagement des parties prenantes** dans le processus de mise en œuvre constitue un deuxième axe stratégique clé de la mise en œuvre. Les acteurs publics sont incontournables à ce propos, qu'il s'agisse des parlementaires chargés des mesures d'insertion de la convention dans le droit national, de l'exécutif en charge de la mise en œuvre des politiques publiques dans les domaines couverts par la convention ou des acteurs de la justice (magistrats, avocats et autres professions juridiques…) en charge du contentieux de l'application. Les acteurs des médias et de la société civile sont également essentiels pour disséminer l'information, sensibiliser et communiquer. Les acteurs privés sont tout aussi importants : entreprises, experts ou autres. Les écoles et universités publiques ou privées peuvent également avoir un rôle important à jouer.

La convention intervient dans un domaine qui exige la collaboration entre les diverses parties prenantes. Sa mise en œuvre gagnerait ainsi à favoriser une approche multi-parties prenantes. Il serait pertinent de mettre à profit le numérique pour créer, autour de la page web déjà évoquée, une plateforme ou un forum continental qui permettrait aux différentes entités de partager leur savoir-faire, de discuter des défis et des opportunités, et de collaborer sur des initiatives conjointes liées aux domaines couverts par la convention.

Le **renforcement des capacités nationales** constitue un troisième axe clé de la mise en œuvre de la convention. Les parties prenantes engagées auront en effet besoin d'être formées et de voir leurs capacités renforcées. Ici encore, le numérique constitue un atout qui pourrait permettre, à travers une plateforme e-learning accessible à partir de la page web dédiée à la convention, de proposer des sessions de formations, webinaires, webconférences à travers tout le continent. Avec d'autres personnalités publiques, privées et sociétales choisies, les personnes formées peuvent devenir des ambassadeurs de la convention qui peut être un titre honorifique avec des engagements de la part des personnes qui le portent. Un partenariat peut être noué avec des écoles, universités et institutions de formation en vue de rendre disponibles les formations accompagnées de supports de formation (audio, vidéo, textes…), de tests et exercices ludiques de mise en pratique. Des certifications pourraient être proposées sous certaines conditions.

L'application effective de la convention exige que les États membres possèdent les compétences et les infrastructures nécessaires pour assurer les transactions électroniques, protéger les données et la sécurité et combattre la cybercriminalité. Les efforts de renforcement des capacités devraient s'étendre aux divers aspects juridiques, techniques, politiques, et organisationnels. Ceci pourrait impliquer le développement de cadres nationaux de l'économie numérique, de protection des données, de cybersécurité, et de lutte contre la cybercriminalité, la formation des professionnels et des décideurs, et l'amélioration des infrastructures et des technologies de l'information et de la communication. Les expériences de différents pays et régions dans la mise en œuvre de politiques dans ces domaines permettraient de capitaliser sur les leçons apprises et les meilleures pratiques en mettant en lumière les stratégies qui ont été particulièrement efficaces, les défis rencontrés et les solutions adoptées pour les surmonter. Il est crucial d'examiner les conditions sous-jacentes qui ont contribué au succès ou aux échecs des initiatives, et comment ces leçons pourraient être appliquées ou adaptées au contexte des autres pays africains.

Mettre à jour la convention au regard des évolutions technologiques et juridiques

La mise à jour de la convention peut constituer une occasion de combler tout d'abord les insuffisances relevées, puis d'intégrer les nouveautés liées aux évolutions technologiques et juridiques.

En vue de **combler les insuffisances**, des modifications pourraient être apportées tendant à :

- changer la dénomination de la convention pour adopter une dénomination plus englobante et actuelle, mettant l'accent sur les besoins de confiance et de sécurité dans le numérique ;

- améliorer le régime juridique de la protection des données personnelles, d'une part, en l'allégeant au mieux des formalités préalables tout en renforçant les responsabilités des responsables de traitement et organisant un contrôle a posteriori plus efficace et, d'autre part, en définissant les critères de l'indépendance de l'autorité nationale de protection qui est centrale dans le succès du dispositif de protection ;
- accorder une place expresse aux transactions administratives et financières de plus en plus développées en Afrique à côté des transactions commerciales pour offrir un cadre général harmonisé des transactions électroniques à l'échelle africaine, surtout dans la perspective d'un marché numérique africain ;
- intégrer dans les dispositions prévues en matière de lutte contre la cybercriminalité des règles de droit international privé permettant de traiter des conflits de lois et de compétence juridictionnelle qui peuvent se poser en matière de cybercriminalité.

Ensuite, dans le but d'**intégrer les nouveautés**, il est essentiel de consacrer, en tenant compte des orientations déjà abordées plus haut, des dispositions relatives aux questions liées :

- à la cyberdéfense et la sécurité nationale en vue de cibler le cyberterrorisme, consacrer de nouvelles infractions ou adapter des existantes à ce type de menaces liées aux infrastructures critiques, logiciels malveillants, désinformation ou exploitation des réseaux sociaux pour le recrutement, l'organisation ou la perpétration d'actes terroristes, donner des orientations sur le cadre institutionnel et les mécanismes à mettre en place ainsi que les mesures de protection des infrastructures critiques, de renforcement des capacités, de collaboration avec le secteur privé et la société civile ou encore la mise en place de cadres juridiques nationaux en matière de cyberdéfense ;
- à l'encadrement de l'intelligence artificielle à travers l'intégration de lignes directrices éthiques et de cadres de gouvernance pour assurer un développement et une utilisation responsable de l'IA, garantissant ainsi que ces technologies bénéficient à tous les citoyens de manière équitable ;
- à l'encadrement du marché et des services numériques africains en cohérence avec l'accélération de la mise en œuvre de la Zlecaf, dans une approche plus globalisante du commerce électronique tel qu'envisagé dans la convention en vigueur, en tenant compte des défis associés tels que la fiscalité numérique et une protection approfondie des consommateurs en ligne, et en consacrant les règles et principes essentiels pour un marché numérique continental africain ouvert, intégré et inclusif ;
- aux droits numériques et à l'inclusion numérique qui nécessitent de s'assurer que tous les groupes de la société ont accès aux technologies numériques et sont capables de les utiliser efficacement, en particulier, les personnes les plus vulnérables, ce qui revient à garantir un accès aux services numériques équitable, sans discrimination basée sur la localisation, les revenus, ou d'autres facteurs en consacrant les divers droits évoqués plus haut dans les dispositions de la convention.

Prévoir un cadre institutionnel et des mécanismes de mise à jour permanente

L'une des insuffisances identifiées dans le cadre de la mise en œuvre de la convention de Malabo est l'absence d'un cadre institutionnel et de mécanismes effectifs de sa mise à jour permanente. Dans le but de tirer les leçons de l'expérience de la convention en vigueur, il serait important de les mettre en place. Le texte et les dispositions devraient ainsi être révisables et modifiables pour s'adapter, notamment, aux nouveaux défis juridiques liés aux technologies émergentes. L'intégration d'un tel mécanisme peut se réaliser à travers des clauses de révision périodique.

L'existence d'un cadre institutionnel de mise en œuvre évoqué plus haut peut faciliter la mise en place de ces mécanismes de mise à jour régulière de la convention. Cette dernière pourrait être confiée à l'organe de suivi et de mise en œuvre composé d'experts reconnus ainsi que des parties

prenantes chargées de faire de la veille technologique et juridique afin de proposer, sur une base périodique définie dans la convention (une périodicité au moins annuelle), les mises à jour destinées à encadrer les phénomènes induits par les évolutions technologiques importantes.

Renforcer la coopération et l'harmonisation régionale et internationale

Enfin, étant donné la dimension transfrontalière de la société et du marché numériques, l'harmonisation des politiques et des réglementations aux niveaux régional et international est impérative. Cela comprend la mise en place de mécanismes de coopération pour le partage d'informations et la mutualisation des ressources. La convention doit devenir un instrument catalyseur, promouvant une approche harmonisée à l'échelle du continent pour relever les défis de la mise en place d'un marché numérique africain et optimiser l'interopérabilité et la cohérence entre les initiatives nationales.

Conclusion

L'entrée en vigueur de la convention de Malabo fait partie de ces événements qui auraient dû compter parmi les faits majeurs que l'on inscrit à l'actif du bilan de l'année 2023 pour l'UA et des États parties. Force est toutefois d'admettre un succès mitigé vu la résonance plutôt discrète de cette entrée en vigueur. Elle est pourtant bienvenue au regard des importants acquis soulignés, à l'image de l'harmonisation qu'apporte la convention à l'échelle africaine ainsi que des orientations en matière de transactions électroniques, de protection des données personnelles, de promotion de la cybersécurité et de lutte contre la cybercriminalité. Certes, des insuffisances importantes ont été relevées en termes de pertinence limitée de certaines dispositions, force contraignante limitée ou encore absence de cadre institutionnel et de mécanismes de mise en œuvre.

Il s'y ajoute que dans un monde numérique dont la vitesse et l'ampleur de l'évolution sont de plus en plus fortes, l'entrée en vigueur tardive de la convention, neuf ans après son adoption, rend impérieuse son actualisation. À cet effet, des enjeux aussi importants que l'intelligence artificielle, le cyberterrorisme et la sécurité nationale, les marchés et services numériques ou encore les droits numériques et l'inclusion numérique nécessitent une prise en charge par la convention.

Avec l'accélération de la mise en place de la Zlecaf, les opportunités et les défis dans le domaine de l'économie numérique vont probablement se multiplier. À l'inverse, l'avenir verra potentiellement l'émergence de nouvelles formes de cybermenaces, mais aussi de nouvelles stratégies et technologies de défense. La capacité de mise à jour permanente de la convention sera ainsi un facteur clé de sa capacité à encadrer efficacement les nouveaux phénomènes.

Aussi est-il essentiel que l'ensemble des parties prenantes, sous la houlette de l'Union africaine, puisse harmoniser les actions nécessaires à une mise en œuvre et un suivi effectifs et dynamiques de la convention de Malabo. Une belle résolution pour l'année 2024 ?