Entry into Force of the Malabo Convention

Beyond the Good News, the Challenges of Implementation and Updating

Boubacar Diallo*
Expert in digital law
Carapaces - Strategies & Compliance
bdiallo@carapaces.net

How to cite this paper:
Diallo, B. (2024). Entry into force of the Malabo Convention: Beyond the good news, the challenges of implementation and updating . Global Africa, (5), pp. 56-70.
https://doi.org/10.57832/57wg-c486

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

Abstract

The Malabo Convention, which officially came into force in 2023 following its ratification by Mauritania, represents a crucial step towards the harmonization of legal frameworks in Africa when it comes to cybersecurity and personal data protection. This legal instrument, adopted by the African Union in 2014, aims to respond to the challenges posed by the rapid evolution of information and communication technologies (ICTs) and to promote regional cooperation in these fields. Despite its significant potential for improving digital security and data governance at the continental level, the article highlights the need for the Convention to be continually updated to incorporate emerging issues such as artificial intelligence and cyberterrorism. It also calls for effective implementation and increased cooperation between African countries to ensure successful legislative harmonization, while taking into account international standards.

Keywords

Malabo Convention, cybersecurity, data protection, digital economy, legislative harmonization, African Union, artificial intelligence, cyberterrorism

*This article was produced as part of the research program “Strengthening Personal Data Protection in Africa (ProDP-Africa)” which is carried out by LASPAD, Gaston Berger University of Saint-Louis.

Introduction

On June 27, 2014, in Malabo, Equatorial Guinea, the Conference of Heads of State and Government of the African Union (AU) adopted the Convention on Cybersecurity and the Protection of Personal Data, known as the "Malabo Convention". Through this legal framework, the AU aimed to define the objectives and set the main directions of the information society in Africa, and to strengthen the legislation of member states and Regional Economic Communities (RECs) in the field of Information and Communication Technologies (ICTs). On May 9, 2023, Mauritania submitted its ratification instrument, the fifteenth[1], thus marking the entry into force of the Convention, in accordance with its article 36, thirty days after it had been received by the Chairman of the AU Commission, i.e., June 8, 2023.

The Convention covers a range of issues, including electronic transactions, personal data protection, cybersecurity promotion and the fight against cybercrimes. With its entry into force, Africa now has its first continental legal instrument designed to harmonize sub-regional, regional and national laws, while taking into account member states' international commitments in the fields of cybersecurity and personal data protection. The drafting process involved a wide range of stakeholders, including legal experts, cybersecurity specialists, government officials and civil society stakeholders, with the aim of integrating diverse perspectives and ensuring that the Convention was both comprehensive and adapted to the specific realities of the continent.

The Convention establishes a common minimum legal framework to guide national and continental efforts in the development of electronic transactions, the fight against cybercrimes, the promotion of resilient cybersecurity, and the protection of human rights through personal data protection. Its entry into force therefore undoubtedly represents a major step forward in establishing the legal and institutional conditions for trust required to develop digital technologies for the benefit of African societies. This is all the more important as, to this day, many AU member states still do not have legal framework in some of the areas covered by the Malabo Convention[2].

It has to be said, however, that in a field as fast-moving as digital technologies, the Convention's entry into force, nine years after its adoption, is long overdue. New technologies have emerged and others, then in their infancy, have reached maturity (artificial intelligence - AI, Big Data, blockchain, 3D printing, IoT...), disrupting many sectors of political, economic, social and cultural, environmental and legal life. New legal issues arising from these innovations do not find adequate answers in the Convention. The AU's strategic framework for data[3] and the assessment of AI needs in Africa[4] also reflect the wide gap between the issues covered by the Convention and the real need to address current issues linked to the digital market and society in Africa.

This is all the more true as the AU has taken new initiatives in the field of Africa's digital transformation, with the aim of bringing about an integrated and inclusive digital society and economy, improving the quality of life of African citizens[5]. This global strategy is led by the African Union Commission, in

1 After Senegal (August 16, 2016), Mauritius (March 14, 2018), Guinea (October 16, 2018), Namibia (February 1, 2019), Ghana (June 3, 2019), Rwanda (November 21, 2019), Mozambique (January 21, 2020), Angola (May 11, 2020), Congo (October 23, 2020), Zambia (March 24, 2021), Togo (October 19, 2021), Cape Verde (February 5, 2022), Niger (March 16, 2022) and Côte d'Ivoire (April 3, 2023). https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_Convention_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf. Accessed on November 8, 2023.

2 To date, according to data from the United Nations Conference on Trade and Development (UNCTAD), only 33 countries (61%) have legislation on electronic transactions and personal data protection, and 39 countries (72%) on cybercrimes: https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide. Accessed on November 8, 2023.

3 See: https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf. Accessed on November 20, 2023.

4 See the survey carried out under the aegis of Unesco: https://unesdoc.unesco.org/ark:/48223/pf0000375322. Accessed on November 20, 2023.

5 In addition to the AU's strategic framework for data precited, see the document "THE DIGITAL TRANSFORMATION STRATEGY FOR AFRICA (2020-2030)": https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf. Accessed on November 20, 2023.

collaboration with the United Nations Economic Commission for Africa (UNECA), Smart Africa, the African Union Development Agency (AUDA-NEPAD), the African Telecommunications Union (ATU), the African Capacity Building Foundation (ACBF), the International Telecommunications Union (ITU) and the World Bank (WB). It intends to build on existing initiatives and frameworks such as the Policy and Regulatory Initiative for Digital Africa (PRIDA), the Program for Infrastructure Development in Africa (PIDA), the African Continental Free Trade Area (AfCFTA), the African Union Financial Institutions (AUFI), the Single African Air Transport Market (SAATM) and the Free Movement of Persons (FMP) to foster the development of the African Digital Single Market (DSM), as part of the African Union's integration priorities. This approach is fully in line with Smart Africa's strategic vision for the creation of a single digital market in Africa.

Moreover, the lack of reliable digital infrastructure, disparities in digital development between countries, and variations in the legal and technical capacity of states have a definite impact on the effective implementation of the Convention across the continent.

So, while we welcome the real progress made by many African countries following the entry into force of the Malabo Convention, it is essential to take an up-to-date look at it, taking into account both new phenomena linked to technological developments and the strategic, institutional and legal frameworks that have enriched the reference frameworks underlying the adoption of the Convention. Such a reading will enable us to identify the areas where updating is already necessary, and to reflect on the obstacles to effective implementation of the Convention. This ambivalence between necessary implementation and imperative updating is the thread of the balance that needs to be highlighted, so that the Convention's entry into force is synonymous with effectiveness, and also enables it to meet the current needs of an integrated and inclusive digital Africa, in an environment that guarantees digital security and trust.

It is indeed crucial to reflect on the essential conditions for the effectiveness and relevance of the Malabo Convention to enable Africa to succeed in its digital transformation strategy.

To this end, taking into account the continent's current context and the issues linked to technological developments, in line with the strategic, institutional and legal orientations defined, it is important to carry out a cross-analysis of the Convention and the strategic and legal documents in the digital field in Africa, such as the Digital Transformation Strategy for Africa (2020-2030), the AU's strategic framework for data or the assessment of AI needs in Africa... In the light of this analysis, the entry into force of the Malabo Convention appears to be both welcome, with gains to be consolidated (I), eagerly awaited despite shortcomings to be remedied (II), and late, given all the new features to be integrated (III). This analysis enables us to formulate strategic recommendations for the future (IV).

A Welcome Entry into Force and Achievements to Be Consolidated

The Malabo Convention focuses on three main areas: (i) the promotion of digital economy through standards for electronic transactions, (ii) the protection of human rights through provisions on personal data protection, and (iii) the promotion and protection of the essential values of an African digital society through provisions on cybersecurity and cybercrime. These provisions are designed to underpin digital security and confidence in Africa. The entry into force of the Convention thus lays the foundations for harmonizing regional and national legal frameworks (A), and for defining guidelines for electronic transactions (B), setting minimum requirements for the protection of personal data (C) and outlining the promotion of cybersecurity and the fight against cybercrimes (D).

 https://doi.org/10.57832/57wg-c486

Harmonizing Regional and National Legal Frameworks

It is worth mentioning that an action framework, the "African Information Society Initiative" (AISI) was launched quite early on, back in 1995, during the African Regional Symposium on Telematics for Development, held in April 1995 in Addis Ababa[6]. Africa's interest in digital technology was thus reflected early on in this initiative, which made harmonization one of its guiding principles. This approach was first manifested by the launch of AISI at the Conference on the Information Society for Africa's Development in May 1996 in South Africa, attended by fifteen African countries, and then by its adoption by various African bodies, notably, the African Ministers of Telecommunications through the African Regional Conference on Telecommunications Development held in Abidjan in 1996, then by the adoption of a declaration on AISI by the Council of Ministers of the Organization of African Unity (OAU) on the occasion of the OAU Summit held in Yaoundé in July 1996. AISI was subsequently integrated into the ECA's work program.

The ECA had in fact initiated a major project to harmonize ICT legislation in cooperation with ECOWAS and WAEMU[7]. As an extension of this convergence process, the African Union's Convention project was launched, with the aim of establishing legal rules to underpin security and confidence in Africa's information society. Africa thus appears as a precursor in the reflection on the evolution towards the information society with the AISI, created in 1995. Indeed, on a global level, it was not until 2003 with the first phase of the World Summit on the Information Society (WSIS) in Geneva (Switzerland) and 2005 with the second phase in Tunis (Tunisia) that the Geneva Declaration of Principles and Action Plan and the Tunis Commitment and Action Plan for the Information Society[8] were adopted. The drafting of the Malabo Convention was fully in line with the African Union's desire to support the establishment of an African information society based on security and trust[9].

The aim of having a harmonized legal framework that takes into account the international and regional commitments of member states is thus strongly affirmed and recalled in the preamble to the Convention[10]. To this end, three major issues had to be taken into account: respect for human rights enshrined in international and African law, development of the digital economy and protection of the fundamental values of the African information society. This explains the extension of the Malabo Convention beyond the fight against cybercrimes, to include personal data protection and electronic transactions.

It is true that, at this point in time when the Malabo Convention has come into force, 33 African countries (61%) already have legislations on electronic transactions and personal data, and 39 countries (72%) have legislations on countering cybercrimes[11]. This means, however, that among the 54[12] African countries recognized by the UN, 28 do not have legislations on electronic transactions and personal data, and 15 have none on combating cybercrimes[13]. The entry into force of the Malabo Convention is good news both for countries that already have legislation and for those that do not. For the former, the Convention represents a minimum foundation enabling countries to ensure

6 The symposium was organized "by the Economic Commission for Africa (ECA), in association with the International Telecommunication Union (ITU), the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the International Development Research Centre (IDRC), who have joined forces in the framework of the African Networking Initiative". See ECA, Implementation of the African Information Society Initiative, Progress Report: https://repository.uneca.org/bitstream/handle/10855/3076/Bib-25638.pdf?sequence=1&isAllowed=y. Accessed on November 27, 2023.

7 This initiative led to the implementation of the additional act A/SA.1/01/10 of February 16, 2010 on the protection of personal data in the ECOWAS region.

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

9 The Convention takes into account : 1) the African Declaration on Internet Governance known as the "Oliver Tambo Declaration" adopted by the African Union Extraordinary Conference of Ministers in charge of Communication and Information Technology in Johannesburg on November 5, 2009; 2) the Declaration on Information and Communication Technologies in Africa: Challenges and Prospects for Development; 3) the Abidjan Declaration adopted on February 22, 2012 and the Addis Ababa Declaration adopted on June 22, 2012 on the harmonization of cyber legislation in Africa.

10 The preamble states that the Convention "aims both to define the objectives and main orientations of the information society in Africa, and to strengthen the existing legislation of member states and regional economic communities (RECs) in the field of information and communication technologies".

11 According to UNCTAD data, see: https://unctad.org/page/e-transactions-legislation-worldwide. Accessed on November 27, 2023.

12 The UN officially recognizes 54 African countries (https://www.un.org/en/about-us/member-states), while the AU officially recognizes 55 (https://au.int/en/member_states/countryprofiles2).

13 This includes countries for which UNCTAD has no data on the existence of such legislation.

that their legislation takes account of the requirements of a legal framework in harmony with the existing continental framework. For the latter, these minimum requirements will enable their future legislation to incorporate *ab initio* the objectives set by the Convention.

The entry into force of the Convention means that Member States are obliged to transpose it into their domestic laws, in order to ensure the uniform level of protection required to ensure digital security and confidence in Africa. This is all the more important as it takes into account the need to comply with the legal frameworks put in place by the RECs, such as ECOWAS, WAEMU and ECCAS. It is also welcome in that it contributes to the consolidation of achievements in the harmonization of national legislations, the laying down of the foundations for electronic transactions, personal data, the promotion of cybersecurity and the fight against cybercrimes.

Defining Guidelines for Electronic Transactions

Digital technologies are a powerful lever for transforming societies and economies. Their transformational impact is unprecedented in terms of speed and scope, and therefore represents a real opportunity for Africa[14]. Aware of these positive prospects, the AU has set itself the ambition of creating a secure digital single market by 2030[15]. What was true when the Convention was adopted in 2014 is even truer today in terms of the importance of developing the digital economy to promote the emergence of conditions for a more prosperous African economy. Africa is a fantastic reservoir of platform and service users: 453 million Africans (out of 1.2 billion) are connected today. This proportion (35%) is set to increase significantly, as the continent's population is set to reach 2.5 billion by 2050[16].

In the face of such challenges, the establishment of an appropriate legal framework is a key factor in ensuring the security and confidence necessary for the development of the digital economy. The investment needs for digital development are excellent indeed, and their realization depends largely on the ability of Africans to put in place the conditions for making such investments. These conditions include the existence of a legal and regulatory framework conducive to the development of the digital economy.

The regulations on e-commerce lay down the basic obligations to be met by any supplier of electronic goods or services[17], while preserving the principle that the supplier's contractual liability is subject to the relevant national regulations[18]. They also provide a framework for advertisements done via electronic means while keeping up with the commitments of the States parties, notably in the field of canvassing. Electronic commerce contracts are also protected by specifying how they are to be concluded, and safeguarding written and electronic proof. This principle thus plays an important role in the Convention, which leaves it up to the States parties to set the legal conditions for it. The measures for securing electronic transactions draw the consequences of the electronic signature for the validity of electronic payment methods, as well as the probative value of documents bearing a qualified electronic signature. Such measures are essential to create the conditions for the existence and development of e-commerce, even if the context and issues at stake have changed considerably, making it necessary to amend the Convention's provisions. They are, however, basic guidelines for national legislation, to which are added minimum requirements for personal data protection.

14 A 10% increase in mobile broadband penetration in low-income economies leads to a 2% increase in GDP. In sub-Saharan Africa, this trend is even more pronounced, as a 10% increase in mobile broadband penetration is expected to lead to a 2.5% increase in GDP. Cf. ITU, 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. Accessed on November 27, 2023.
15 Cf. Digital Transformation Strategy for Africa (2020-2030), op. cit.
16 M. Olivier and S. Ballong, "Gafam: l'Afrique face aux géants du Web", report published on August 16, 2018.Cf. https://www.jeuneafrique.com/mag/614444/societe/gafam-lafrique-face-aux-geants-du-web/. Accessed on January 29, 2024.
17 Cf. in particular, art. 2 of the Convention, which sets out the mandatory information and mentions it to be respected.
18 Cf. art. 3 of the agreement.

Setting Minimum Requirements for the Protection of Personal Data

In the Convention, the African Union reiterates its commitment to international and African undertakings to protect human dignity and the human rights that derive from it. In the digital age, personal data shared by users is a constant source of concern for the preservation of individual dignity, confidentiality and, more broadly, the protection of their rights. For this reason, the Convention reiterated that the protection of personal data and privacy is a major challenge for the information society, both for public authorities and for other stakeholders. It considers that this protection requires a balance between the use of ICTs and the protection of citizens' privacy in their daily or professional lives, while guaranteeing the free flow of information.

Underlining the commitment of States to the establishment of a legal framework for the protection of personal data, the Convention imposes, depending on the case, a formal procedure of preliminary declaration or authorization. It also devotes significant provisions to the institutional framework that each State party must put in place to protect such data. The responsibilities of these national authorities are specified, as are their powers. From a substantive point of view, the Convention lays down the principles to be respected in the processing of personal data, specifying the very rules that govern sensitive data or the interconnection of files containing these types of data, as well as the rights of the owners of the personal data processed and the obligations of the data controller.

Data protection regulations thus establish safeguards to ensure that citizens' personal information is handled securely and ethically. As a result, they provide a framework that guarantees greater security and safeguards citizens' privacy in the digital space. Provisions relating to cybersecurity and the fight against cybercrimes reinforce this security framework.

Shaping the Framework for the Promotion of Cybersecurity and the Fight against Cybercrimes

When we talk about the opportunities offered by digital technology, we cannot ignore the significant risks it also entails. Promoting the development of a secure digital market in Africa presupposes the existence of a trustworthy legal framework.

For this reason, the African Union understood the urgent need to put in place, through the Convention, a mechanism to address the dangers and risks arising from the use of computers and files on individuals, with a view to respecting privacy and freedoms, while encouraging the promotion and development of ICT in its member countries. The promotion of cybersecurity and the fight against cybercrimes thus play a central role in the Convention.

The implementation of harmonized cybersecurity legislation in AU member states therefore required the adoption of minimum legal rules enabling states, public, private and societal organizations, as well as individuals within them, to be aware of the risks and protect themselves against the multiple infringements of users' rights, information infrastructures and systems, data, etc. that digital technology entails. When such attacks jeopardize the essential values of society and the market, criminal-law protection of the value system of the information society becomes a necessity, through provisions devoted to the fight against cybercrimes.

Taking into account the commitments made by States at sub-regional, regional and international levels, the Convention sets out the main lines of the strategy to combat cybercrimes, in order to protect computer networks and the information society from cybercriminal threats.

To this end, from the point of view of substantive criminal law, the aim of the Convention was to modernize the instruments used to repress cybercrimes. On the one hand, new incriminations specific to ICTs have been established to deal with the new criminal phenomena brought about by these technologies. On the other hand, existing offenses have been adapted, as have the penalties and criminal liability systems in force in the Member States, to bring them into line with the specific features of the information and communication technology environment. Apart from certain offenses against property, the most important innovation in this area concerned the criminal liability of legal entities, which the Convention requires States Parties to make effective in their domestic law.

In terms of procedural criminal law, the same approach was adopted: on the one hand, to institute new procedures specifically for cybercrimes, insofar as existing procedures were unable to deal with phenomena linked to the technologies in question, and on the other, to adapt existing procedures to information and communication technologies.

The aim of this scheme to promote cybersecurity and combat cybercrimes was to secure cyberspace in Africa as an essential prerequisite for digital economic development. With the ambition of creating a secure and regulated digital environment, the Malabo Convention also aimed to encourage the investment needed for development in the digital sector by promoting technological innovation. The Convention's entry into force will undoubtedly contribute to this, and for this reason was eagerly awaited, despite the shortcomings that remain to be remedied.

An Expected Entry into Force but Shortcomings to be Remedied

The entry into force of the Malabo Convention was expected to provide a harmonized legal framework for personal data protection, electronic transactions, cybersecurity promotion and the fight against cybercrimes. However, as soon as it was adopted, a number of shortcomings became apparent, some of which can be considered to be inherent to the adoption process, as well as to the legal nature of the Convention. The questionable relevance of certain provisions (A), its limited binding force (B), the lack of an institutional framework for implementation (C), and the absence of permanent mechanisms for updating (D) the Convention are all shortcomings that need to be remedied.

Questionable Relevance of Some of the Regulations

The "misnamed" African Union Convention on Cybersecurity and Personal Data Protection also deals with electronic transactions and cybercrimes. This is a very simplistic title, as it does not cover all the legal issues involved in the above-mentioned triple challenge. Some of the titles of the initial draft were more relevant and encompassing, as they positively emphasized the need for trust and security in the information society, which the Convention was intended to address[19]. Emphasizing the need for trust and security in the digital world not only encompasses all the issues addressed by the Convention, but also presents it as a means of meeting these essential needs for States, public, private and societal organizations, as well as individuals and all stakeholders in a digital society and market. But beyond its name, other provisions of the Convention are of questionable relevance.

In particular, the relevance of some data protection regulations may be called into question. Apart from exceptional cases, they provide for prior declaration or authorization formalities (article 10), depending on the case, which may seem cumbersome to implement given the number of processing systems used in an increasingly digital society. A system that makes data controllers more accountable and organizes more effectively a posteriori control might be more appropriate. They also stipulate that the personal data protection authority must be an independent authority (article 11), but without defining the criteria for this independence, which is central to the success of the protection system.

Other provisions on electronic transactions may also raise questions about their relevance, in particular their ability to regulate administrative and financial transactions, which are increasingly developing in Africa, as well as commercial transactions, which seem to be the only ones really covered. Of course, other authorities, notably regional or national (regional or national central

19 A "draft African Union Convention on the establishment of a trusted legal framework for cybersecurity in Africa" is still available online. The version of the Convention published on the website of Senegal's Commission de protection des données personnelles (CDP) is indeed entitled "Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel" (African Union Convention on Cybersecurity and Protection of Personal Data), on the title page, but in Article 1 devoted to definitions appears for "(The present) Convention", "Convention de l'Union africaine sur la confiance et la sécurité dans le cyberespace" (African Union Convention on Trust and Security in Cyberspace). No doubt the CDP publication will soon be withdrawn, but it is to be hoped that this archive will be preserved not only for the sake of memory, but also for the greater relevance of the title it proposes. See project: https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf. Accessed on November 28, 2023.

banks or banking commissions and financial market authorities) are competent to regulate these transactions, but the Convention can offer a general framework harmonized on an African scale, especially in the perspective of an African digital market. Finally, the provisions on combating cybercrimes do not include rules of private international law to deal with the conflicts of law and jurisdiction that may arise in cybercrime cases. These shortcomings add to the limited binding force of the Malabo Convention, despite its entry into force.

Limited Binding Force of the Convention

The entry into force of the Malabo Convention makes it applicable to all member states. Its applicability does not, however, mean that litigants in the member states can directly invoke its provisions, in particular against national authorities. The Malabo Convention has no direct effect. Nor does it have any immediate effect, as it requires each State party to take the legal and regulatory measures needed to transpose its provisions into domestic law.

Despite its entry into force, the binding force of the Convention remains very limited, given the need for action by the States Parties to ensure that its provisions are applicable in domestic law. The means of "convincing" member states to adopt such provisions are also very limited, in the absence of effective sanctions. As mentioned above, many countries do not yet have legislation in the areas covered by the Convention, and litigants in these countries are thus exposed to the phenomena of the digital society and market. Yet these provisions would provide them with a minimum legal framework for the economy, personal data protection, cybersecurity and the fight against cybercrimes.

The lack of an institutional framework for implementing the Convention at AU level means that the shortcomings associated with its limited binding force cannot be overcome.

Lack of an Effective Institutional Framework for Implementation and Monitoring

The adoption of the Malabo Convention was not accompanied by the establishment of an effective institutional framework for its implementation. It is true that Article 32 lays down follow-up measures to be taken at AU level, but the ineffectiveness of such measures has prevented certain issues from being properly addressed.

The team of experts who designed and drafted the Convention[20] proposed and envisioned the effective establishment of an institutional framework for its implementation, with an approach linked to the RECs. Based on pre-existing regional texts, notably those of ECOWAS[21], the proposed ratification strategy relied on an institutional mechanism for monitoring ratifications linked to this REC, whose member states already had domestic legal texts at least equivalent to a transposition of the Convention's provisions. There is no doubt that such an institutional approach would have shortened the time needed for the Convention to enter into force.

The resource people behind the conception and adoption of the Convention could have been involved through such an institutional framework. They could also have been reinforced by new African skills and expertise. It would also undoubtedly have made it possible to offer member states assistance, in terms of expertise and capacity building in such a technical and high-stakes field, with the aim of speeding up the formal adoption and transposition processes into national law.

Lack of Permanent Updating Mechanisms

The speed and scale of expansion of new technologies have increased exponentially. Launched in 1878, the telephone took seventy-five years to reach 100 million users. This time was reduced to sixteen years for the cell phone launched in 1979. It took four years and six months to Facebook after

20 See A. Cissé, "La Convention de Malabo, l'impérieuse actualisation!", paper delivered at the Laspad "Samm sunuy données" session.
21 See Additional Act A/SA.1/01/10 of February 16, 2010 on the protection of personal data in the ECOWAS region, op. cit.

its launch in 2004 while Whatsapp, launched in 2009[22], only needed three years and four months to do it, ChatGPT[23] was launched in 2022 and achieved it in sixty days. Threads broke the record, reaching 100 million users[24] in five days after its launch in July 2023.

In a digital world where technology is evolving at a lightning pace, the Convention must be flexible and adaptable to the new realities and challenges of cyberspace. This means that the text and related terms should be revisable and modifiable to adapt, in particular, to new legal challenges related to emerging technologies. Incorporating a mechanism that allows for periodic review and updating is vital to ensure that it remains relevant and effective in the face of changing challenges and dynamics in the digital society and market.

While the Convention provides for an amendment or revision mechanism (article 37), as well as the aforementioned monitoring mechanisms (article 32) included in the Convention do not appear to be suitable for updating it regularly in a way that can match digital developments. As envisaged, amendments or revisions are submitted by any of the member States, which means that the initiative lies with them.

The existence of the institutional framework mentioned above could have facilitated the establishment of regular update mechanisms. This could be entrusted to the monitoring and implementation body, made up of recognized experts in the field. Stakeholders could be responsible for monitoring technological and legal developments in order to provide, on a periodic basis defined in the Convention (at least once a year), updates targeting disruptive changes brought by major technology progress. The amendment process could then be laid down in the agreement to undoubtedly avoid the need for an update as soon as the agreement came into force.

A Late Entry Into Force and New Features to be Integrated

The speed and scale of technological developments and the phenomena they bring with them have made many legal regulations obsolete, and they are constantly being overtaken by digital realities. Many new phenomena have emerged since the Convention was adopted. Its late entry into force makes it imperative to update it, particularly with regard to cyberterrorism and national security (A), the ethics and governance of AI and emerging technologies (B), the regulation of digital markets and services in Africa (C), and the issue of digital rights and inclusion in Africa (D).

Cyberterrorism and National Security

The Malabo Convention's goal was to establish a legal framework for promoting cybersecurity and tackling cybercrimes. By the time it came into force, new risks had emerged in a way giving threats a new dimension. Cybercrime attacks are increasingly targeting critical infrastructures and strategic national interest. New forms of digital warfare are emerging, posing significant risks to national defense.

So, while the Convention made a point of addressing various aspects of cybersecurity and cybercrimes, closer attention must be given to the implication of cyberterrorism, particularly in terms of national security. Cyberterrorist attacks, which target critical infrastructures, can have disastrous repercussions not only on the economy, but also on the socio-political stability of member states. A detailed analysis of current and potential threats, combined with the development of robust and appropriate strategies to counter these threats, is essential.

With this in mind, the Convention could incorporate new specific provisions to target cyberterrorism, enshrine new offenses or adapt existing offenses to this type of threat linked to critical infrastructures, malware, disinformation or the exploitation of social networks for the recruitment, organization or

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

perpetration of terrorist acts. It could also provide guidance on the institutional framework and mechanisms to put in place, as well as measures for protecting critical infrastructures, for capacity building, for collaborating with the private sector and civil society, and for establishing national legal frameworks to reinforce cyber defense systems.

It would also be advisable to integrate mechanisms for enhanced sub-regional, regional and international cooperation to ensure effective exchange of information and practices in the fight against cyberterrorism.

Respect for human rights and civil liberties must be at heart of the design and implementation of these measures to ensure effective security against the threats of cyberterrorism.

Ethics and Governance of AI and Emerging Technologies

The rise of artificial intelligence (AI) and other emerging technologies presents considerable ethical and governance challenges that seem to lie beyond the scope of the current Convention. The use of AI in various sectors (security, health, education, migration, etc.) raises multiple questions, linked to essential principles for ethical and responsible AI, which require careful exploration. An update of the Convention could enable the integration of ethical guidelines and governance frameworks to ensure the responsible development and use of AI, thereby guaranteeing that these technologies benefit all citizens in an equitable manner.

In order to take into account, the complexity of the governance of AI and emerging technologies, which needs a multidimensional approach, the guidelines for updating the Convention should include key principles and rules governing their design and implementation like:

- **transparency and accountability** to ensure that AI processes and decisions are transparent. Developers and users of these technologies will therefore be accountable for their actions and the results they will produce;
- **fairness and non-discrimination**, so that AI is designed and used in a way avoiding bias and discrimination and making sure too that, at levels of race, gender, age or other, ongoing efforts are taken to ensure that AI systems treat all users fairly;
- **reliability and safety** of AI systems, to enable them to function as intended and be protected against manipulation and abuse;
- **interoperability**, so that AI systems are able to work with other systems and technologies, while respecting established standards and protocols;
- **responsible innovation**, to encourage innovation while ensuring that technological developments are ethical and aligned with human values and societal well-being;
- **privacy and data protection** as top priorities, which implies robust security measures and compliance with data protection legislation;
- **Inclusion and accessibility** of AI to all, regardless of economic capacity, geographical location, disability, etc., which implies designing inclusive technologies and guaranteeing equitable access;
- **human well-being and social impact** so that AI is developed and used in a way that promotes human well-being, taking into account social, economic and cultural impacts;
- **dialogues and stakeholders participation** for AI governance should include open talks with various stakeholders, including civil society, the public, ethics experts, industry, and governments;
- **sub-regional, regional and international cooperation,** which is essential since, given the cross-border nature of AI and emerging technologies, it is key to developing harmonized standards and rules;

- **education and awareness** because it is important to not only train but also educate all people involved (public, private and societal players, developers, users) on the issues, opportunities and risks associated with AI;
- **adaptability and flexibility**, since AI regulations and policies must be flexible enough to adapt to rapidly evolving technologies;
- **respect for the environment**, so that emerging technologies are developed and used in line with SDG principles.

Such principles and rules could constitute guidelines that would also be adapted to specific contexts and technological developments. They would be a basic framework for ethical and responsible governance of emerging technologies like AI.

Regulation of African Digital Markets and Services

The African Union's ambition to create an integrated and inclusive digital economy in Africa presupposes the creation of a dynamic and prosperous continental digital market. From this point of view, the establishment of AfCFTA represents a real opportunity, as it would "create a continental market of 1.3 billion people with a combined GDP of $3.4 trillion, making it the world's largest free trade area since the creation of the World Trade Organization.... AfCFTA is expected to boost intra-African trade by 52.3% by 2025, to increase Africa's income to $450 billion by 2035, according to the IMF[25], and thus to lift 30 millions of Africans out of extreme poverty"[26]. The digital marketplace in particular, given the opportunities it offers and the large spread of technology in lot of areas, can unlock "the potential of digital commerce in Africa and enable businesses, particularly small and medium-sized enterprises, to reach new markets[27]".

Updating the Convention could provide an opportunity to put in place an appropriate framework for this African digital market, in line with the accelerated implementation of the AfCFTA. Such framework would make it possible to integrate a more global approach to e-commerce, as envisioned in the current Convention, taking into account externalities associated with these challenges such as digital taxation and enhanced online consumer protection. Above all, it would enshrine essential rules and principles for an open, integrated and inclusive continental African digital market.

One of the pillars of such a market should be the organization of free and healthy competition between its various players. To this end, rules and principles enshrined by the AU, through the Convention, should help prevent anti-competitive practices and ensure an open and fair digital market for small and large businesses alike. Fair market access is necessary, in the context of an ultra-dominant global digital market dominated by mega-platforms on which thousands of professionals depend. Rules have to make sure that large platforms don't use their dominant position to discriminate against certain businesses or consumers, or to favor their own services or products. Technology companies must be transparent about their algorithms, data collection policies and business practices. Accountability for content published and actions taken online is crucial. Digital platforms must be held accountable for the content they host, with regulations that balance freedom of expression with the fight against hate speech, misinformation and illegal content.

Rules designed to frame an African digital market should also promote the protection of copyright and intellectual property to encourage innovation and protect creators. They should also encourage digital companies to be mindful of their environmental impact, particularly in terms of energy consumption and electronic waste.

Particular attention should also be devoted, on the one hand, to protecting consumers against abusive or misleading practices while encouraging innovation and, on the other hand, to digital workers with a view to protecting their specific rights, including platform workers and remote workers.

25 International Monetary Fund.
26 Cf. "Zlecaf: Saisir les opportunités pour une Afrique prospère", in Afrique Renouveau, May 2023, by Ms. Nardos Bekele-Thomas, Director General of AUDA-NEPAD, the AU's development arm: https://www.un.org/africarenewal/magazine/may-2023/afcfta-seizing-opportunities-prosperous-africa.
27 Op.cit.

 https://doi.org/10.57832/57wg-c486

Implementing all these principles and rules requires close collaboration with the various institutions involved in economic development on an African scale (UNECA, AfCFTA, AUDA-NEPAD...), those involved in the digital field (Smart Africa, etc.), with international institutions, RECs, governments, technology companies, civil society and users to create a balanced and sustainable digital environment.

Digital Rights and Digital Inclusion

Following on from the implementation of regulations dedicated to the digital market and services in Africa, it is important to devote particular attention to digital inclusion and digital rights. In an African context, it is essential to ensure that all groups in society have access to digital technologies and are able to use them effectively, especially the most vulnerable. Access to digital services should be equitable, without discrimination based on location, income or other factors.

Various rights should be included and guaranteed by the provisions of the Convention. The Convention already affirms its commitment to respecting human rights, and some aspects already taken into account could be developed further. It is imperative to consider universal access to the Internet as fundamental to achieve digital and social inclusion of all citizens. The Convention should therefore promote strategies and policies aimed at guaranteeing fair and affordable access to the Internet, while protecting users' digital rights.

Specifically, there are rights that should be enshrined, including (i) the right to data portability, whereby users could easily transfer their data from one platform to another to foster competition, (ii) the right to repair, which would encourage the sustainability of digital products, reduce e-waste and promote a more sustainable economy.

Education and awareness-raising are, in this respect, an important dimension. Educating consumers and businesses about their rights and responsibilities is crucial for a healthy competitive environment in Africa's digital marketplace.

Finally, it is essential to address the issue of digital rights and digital inclusion at the level of states, companies and individuals alike. It is important that the most digitally excluded countries in Africa receive special attention.

Strategic Recommendations for the Future

Now that the Malabo Convention is officially in force, it is essential to ensure that the conditions for its implementation are met through appropriate accompanying measures (A). The imperative need to update the Convention (B), particularly in light of major technological developments, should not blind us to its usefulness for many African countries, despite the shortcomings identified. Drawing lessons from this first version, we can better prepare its future through an institutional framework and permanent update mechanisms (C) for the next version, while strengthening regional and international cooperation and harmonization (D) following other continent-wide projects and programs.

To Put in Place Measures to Support the Entry Into Force of the Convention

Accompanying the implementation of the Malabo Convention requires a clear strategy involving awareness-raising and communication, stakeholder commitment and national capacity-building.

Awareness-raising and **communication** are the first key strategic axes in the implementation of the Convention, enabling the dissemination of correct information to the relevant targets. In this respect, a range of measures could be envisaged. It is essential to go digital by creating a website dedicated to the Convention, as well as specific accounts and pages on the main social networks used on the continent. These digital tools can be used to build awareness and information campaigns focusing on clear messages about the Convention. A range of AI-enhanced tools can make this

content available on a variety of media (written, audio, video, interactive games, etc.) in different languages, including national ones. Other tools (surveys, feedback, analysis of participation data, etc.) can be used to measure impact. Handbooks, brochures and other communication materials can also be developed for certain key players or for the general public.

Stakeholders involvement in the implementation process is a second key strategic focus. Public players are essential in this respect, whether they are members of parliament responsible for measures to incorporate the Convention into national law, the executive responsible for implementing public policies in the areas covered by the Convention, or the judiciary (magistrates, lawyers and other legal professionals, etc.) in charge of disputes concerning its application. The media and civil society players are also essential for disseminating information, raising awareness and communicating. Private sector is just as important. Schools and universities can also play a major role.

The Convention operates in an area that requires collaboration between the various stakeholders. Its implementation would then benefit from favoring a multi-stakeholder approach. It would be appropriate to create, around the website already mentioned, a continental platform or forum that would enable the various entities to share their know-how, discuss challenges and opportunities, and collaborate on joint initiatives linked to the areas covered by the Convention.

National capacity building is a third key area for the implementation of the Convention. The stakeholders involved will need training and capacity-building. Here again, digital technology is an asset that could be used to offer training sessions, webinars and web conferences across the continent, via an e-learning platform accessible from the Convention's dedicated website. Together with other selected public, private and societal figures, the trainees could become kind of ambassadors for the Convention, with commitments on the part of the bearers. Partnerships can be forged with schools, universities and training institutions to make training courses available, accompanied by training resources (audio, video, texts, etc.), tests and practical exercises. Certifications could also be offered under certain conditions.

Effective implementation of the Convention requires member states to have the necessary skills and infrastructures to ensure electronic transactions, protect data and security, and combat cybercrimes. Capacity-building efforts should be extended to the various legal, technical, political and organizational aspects. This could involve the development of national frameworks for the digital economy, data protection, cybersecurity and the fight against cybercrimes, the training of professionals and decision-makers, and the improvement of information and communication infrastructures and technologies. The experiences of different countries and regions in implementing policies in these areas would enable us to capitalize on lessons learned and best practices, highlighting the strategies that have been particularly effective, the challenges encountered and the solutions adopted to overcome them. It is crucial to examine the underlying conditions that have contributed to the success or failure of initiatives, and how these lessons might be applied or adapted to the context of other African countries.

Updating the Agreement in Line with Technological and Legal Developments

Updating the agreement may provide an opportunity to remedy any shortcomings identified, and to incorporate new features arising from technological and legal developments.

Firstly, in order **to remedy shortcomings**, amendments could be made to:

- change the name of the Convention to a more encompassing and up-to-date one, emphasizing the need for trust and security in the digital world;
- improve the legal framework for personal data protection, on the one hand by lightening the burden of prior formalities while reinforcing the responsibilities of data controllers and organizing more effective 'a posteriori' control, and on the other hand by defining the criteria for the independence of the national data protection authority, which is central to the success of the protection system;

- give an explicit place to administrative and financial transactions, which are increasingly developed in Africa alongside commercial transactions, in order to offer a harmonized general framework for electronic transactions on an African scale, especially in the perspective of an African digital market;
- include the rules of private international law in the planned measures to fight cybercrimes to be able to deal with conflicts of law and jurisdiction that may arise in cybercrime cases.

Secondly, in order **to incorporate the latest developments**, it is essential, taking into account the guidelines already discussed above, to include provisions on issues related to:

- cyber-defense and national security, with a view to targeting cyber-terrorism, establishing new offenses or adapting existing ones to this type of threat, linked to critical infrastructures, malware, disinformation or the exploitation of social networks for the recruitment, organization or perpetration of terrorist acts; providing guidelines on the institutional framework and mechanisms to be put in place, as well as measures for the protection of critical infrastructures, capacity-building, collaboration with the private sector and civil society, and the establishment of national legal frameworks for cyber-defense;
- the regulation of artificial intelligence through the integration of ethical guidelines and governance frameworks to ensure the responsible development and use of AI, thus guaranteeing that these technologies benefit all citizens in an equitable manner;
- the framing of the African digital market and services in line with the accelerated implementation of the AfCFTA, in a more global approach to e-commerce as envisaged in the current Convention, taking into account associated challenges such as digital taxation and enhanced online consumer protection, and enshrining the essential rules and principles for an open, integrated and inclusive continental African digital market;
- digital rights and digital inclusion, which involves ensuring that all groups in society have access to digital technologies and are able to use them effectively, particularly the most vulnerable. This means guaranteeing equitable access to digital services, without discrimination based on location, income or other factors, by enshrining the various rights mentioned above in the provisions of the Convention.

Planning for an Institutional Framework and Permanent Updating Mechanisms

One of the shortcomings identified in the implementation of the Malabo Convention is the absence of an institutional framework and effective mechanisms for its ongoing updates. In order to learn from the experience of the current Convention, it would be important to put these in place. In this way, the text and its regulations can be revised and amended to adapt to the new legal challenges posed by emerging technologies. Such mechanisms could be incorporated through periodic review clauses.

The existence of an institutional implementation framework, as mentioned above, can facilitate the implementation of such mechanisms for regular updating of the Convention. The latter could be entrusted to the monitoring and implementation body, made up of recognized experts as well as stakeholders responsible for technological and legal monitoring, in order to propose, on a periodic basis defined in the agreement (at least once a year), updates designed to provide a framework for the phenomena induced by major technological developments.

Strengthening Regional and International Cooperation and Harmonization

Finally, given the cross-border dimension of the digital society and market, the harmonization of policies and regulations at regional and international levels is imperative. This includes setting up cooperation mechanisms for sharing information and pooling resources. The Convention must become a catalyst, promoting a harmonized continent-wide approach to the challenges of building an African digital market and optimizing interoperability and coherence between national initiatives.

Conclusion

The entry into force of the Malabo Convention is one of those events that should have been one of the major achievements of 2023 for the AU and its member states. However, we have to admit to a mixed success, given the rather discreet resonance of this entry into force. It is nonetheless welcome in view of the major achievements highlighted, such as the harmonization brought about by the Convention on an African scale, as well as the guidelines on electronic transactions, personal data protection, the promotion of cybersecurity and the fight against cybercrimes. Admittedly, significant shortcomings have been noted in terms of the limited relevance of certain provisions, their limited binding force, and the absence of an institutional framework and implementation mechanisms.

What's more, in an increasingly fast-paced and far-reaching digital world, the Convention's late entry into force, nine years after its adoption, makes it imperative that it be updated. To this end, issues as important as artificial intelligence, cyberterrorism and national security, digital markets and services, digital rights and digital inclusion need to be addressed by the Convention.

As the implementation of AfCFTA accelerates, opportunities and challenges in the digital economy are likely to multiply. Conversely, the future will potentially see the emergence of new forms of cyber threats, as well as new defense strategies and technologies. The Convention's ability to be constantly updated will therefore be a key factor in its ability to provide an effective framework for new phenomena.

It is therefore essential that all stakeholders, under the leadership of the African Union, harmonize the actions required for effective and dynamic implementation and monitoring of the Malabo Convention. A great resolution for 2024?