**AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION**

*Federica Cristani\**

# 1. Introduction and short overview of the instrument

The African Union (AU)[[1]](#footnote-1) adopted the AU Convention on Cyber Security and Personal Data Protection (known as Malabo Convention) in June 2014.[[2]](#footnote-2) The Convention entered into force quite recently, on 8 June 2023,[[3]](#footnote-3) becoming the first binding regional treaty on data protection outside Europe.

As stated in the Preamble, "the goal of this Convention is to address the need for harmonized legislation in the area of cyber security in Member States of the African Union, and to establish in each State party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use".[[4]](#footnote-4)

The Convention is built up as a framework convention, providing general rules in three main areas of interest: electronic commerce; personal data protection; and cybersecurity.

In particular, the Convention is structured as follows: Chapter 1 deals with electronic transactions (including provisions for the contractual liability of the provider of goods and services by electronic means, electronic contracts and security of electronic transactions); Chapter 2 deals with personal data protection (including provisions for the establishment of the National Personal Data Protection Authorities, the basic principles that should govern the processing of personal data and the obligations of the personal data controller); lastly, Chapter 3 deals with cybersecurity and cybercrime (including provisions on which cybersercurity measures should be taken at the national level).

It is worth recalling that the AU Convention comes into force when also the African Continental Free Trade Area (AfCFTA) Agreement[[5]](#footnote-5) is already in force. Given that trade and data protection are interlinked, the AU Convention will surely help to implement the goals of AfCFTA. Indeed, the flow of people, goods, and capital throughout Africa requires extensive processing of personal data across borders.[[6]](#footnote-6) The AU Convention can help in efficiently implementing the AfCFTA in this respect.[[7]](#footnote-7)

# 2. Human rights addressed

When it comes to the protection of personal data, Section I of Chapter I of the Convention makes it clear that "[e]ach State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data" (article 8 of the Convention). The following Section IV is then dedicated to the set of rights connected to **data protection**; more in particular, it focuses on

* **Right to information** (article 16)
* **Right of access** (article 17)
* **Right to object** (article 18)
* **Right of rectification or erasure** (article 19)

Also Chapter III of the Convention (Promoting Cyber Security and Combating Cybercrime) exprelly states that "[i]n adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples‟ Rights, and other basic rights such as **freedom of expression, the right to privacy** and the **right to a fair hearing**, among others" (article 25).

# 3. Challenges in the adoption and implementation

The Convention entered into force only nine years after its adoption – and still, only 15 states (among the 55 states of the AU) have ratified it.

Though the entry into force of the Convention should be welcome as a success for the AU, the fact that states have been slow in signing and ratifying it actually hinders the timely achievements of its objectives – like the harmonization of the relevant regulations at the national level in the areas of electronic commerce, data protection, and cybersecurity.

On the other hand, the Convention has had the beneficial effect to increase policy and regulatory awareness on data protection and cybersecurity. For example, after the adoption of the Convention, about 40 States of the AU started to adopt laws on cybersecurity, while about 20 States established national cybersecurity policies, and 18 States adopted national CERT frameworks.[[8]](#footnote-8)

The adoption of the Convention in the framework of the AU brings another beneficial effect, namely the possibility to apply the AU sanction mechanisms against AU Member States that do not comply with the obligations included in the Convention. Indeed, according to article 23, paragraph 2 of the Constitutive Act of the AU, "any Member State that fails to comply with the decisions and policies of the Union may be subjected to other sanctions, such as the denial of transport and communications links with other Member States, and other measures of a political and economic nature to be determined by the Assembly".[[9]](#footnote-9) Since the AU Cybersecurity Convention can surely be considered a decision and policy of the AU, article 23 of the Constitutive Act of AU can apply. However, it should be highlighted that to date, the AU has refrained from adopting sanctions for promoting the implementation of international instruments at the national level among its Member States.[[10]](#footnote-10)

At the same time, a number of challenges make the implementation of the obligations of the AU Cybersecurity Convention difficult to achieve. We can recall, for example, the general lack of expert personnel in AU member states that can facilitate the implementation of national policy and regulatory frameworks for cybersecurity governance, together with the general lack of institutional capacities at the national level in terms of cybersecurity governance and cybercrime law enforcement. For example, law enforcement authorities in many AU member states do not have the capacities to investigate and prosecute cybercrime.[[11]](#footnote-11)

# 4. Similar initiatives elsewhere

The AU Convention replicates several provisions that are included in the Council of Europe´s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[[12]](#footnote-12) and in the European Union´s General Data Protection Regulation.[[13]](#footnote-13)

A number of AU memebr states have also ratified Convention 108+, including Cape Verde, Mauritius, Morocco, Senegal, and Tunisia; some of them have also already included EU privacy-related standards in their national regulations, like the Mauritius.[[14]](#footnote-14) This is what has been described as the "Brussels effect".[[15]](#footnote-15)

# 5. Recommendations

According to Article 32 of the AU Convention, a monitoring mechanism for the Convention should be established, with the following tasks:

"a) Promote and encourage the Continent to adopt and implement measures to strengthen cyber security in electronic services and in combatting cybercrime and human rights violations in cyberspace;

b) Gather documents and information on cyber security needs as well as on the nature and magnitude of cybercrime and human rights violations in cyberspace;

c) Work out methods for analysing cyber security needs, as well as the nature and magnitude of cybercrime and human rights violations in cyberspace, disseminate information and sensitize the public on the negative effects of these phenomena;

d) Advise African governments on the way to promote cyber security and combat the scourge of cybercrime and human rights violations in cyberspace at national level;

e) Garner information and carry out analyses of the criminal behaviour of the users of information networks and computer systems operating in Africa, and transmit such information to competent national authorities;

f) Formulate and promote the adoption of harmonized codes of conduct for the use of public officials in the area of cyber security;

g) Establish partnerships with the Commission and the African Court on Human and Peoples‟ Rights, the African civil society, and governmental, intergovernmental and non-governmental organizations with a view to facilitating dialogue on combating cybercrime and human rights violations in cyberspace;

h) Submit regular reports to the Executive Council of the African Union on the progress made by each State Party in the implementation of the provisions of this Convention;

i) Carry out any other tasks relating to cybercrime and breaches of the rights of individuals in cyberspace as may be assigned to it by the policy organs of the African Union".[[16]](#footnote-16)

The monitoring mechanism has not been established – it remains to be seen how state parties will implement its important section of the Convention.

As already outlined, the implementation of the AU Conventions presents several challenges. To address these challenges, it would be essential to focus on the same key issues, such as strengthening the national legal and regulatory frameworks of AU member states, while at the same time enhancing their technical and infrastructural capacities. Focusing on capacity building and raising awareness can help in overcoming the challenges of the implementation of the AU Convention and can promote harmonization and cross-border cooperation among states.[[17]](#footnote-17)

1. \* Federica Cristani is Head of the Centre for International Law, Institute of International Relations, Prague, and Visiting Senior Researcher at the Arctic Centre of the University of Lapland. E-mail: cristani@iir.cz.

 The African Union (AU) is a regional organization; established in 2002 to replace the Organization of African Unity, it has its headquarters in Addis Ababa. Currently, the AU comprises 55 African States. More information are available at the officiail website: <https://au.int/en/overview>. [↑](#footnote-ref-1)
2. African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014, available at <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>. [↑](#footnote-ref-2)
3. After Mauritania’s ratification on 9 May 2023. According to article 36, the Convention could enter into force thirty days after the date of receipt of the fifteenth instrument of ratification. [↑](#footnote-ref-3)
4. Preable of the Convention. For a general overview of the Convention, see, among others, Uchenna Jerome Orji, The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?, 12(2) Masaryk University Journal of Law and Technology (2018), <https://doi.org/10.5817/MUJLT2018-2-1> and Yohannes Eneyew Ayalew, The African Union’s Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?, EJIL: Talk! Blog (June 15, 2023), <https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/?utm_source=mailpoet&utm_medium=email&utm_campaign=ejil-talk-newsletter-post-title_2>. [↑](#footnote-ref-4)
5. The AfCFTA entered into force on 30 May 2019 and is the world’s largest free trade area bringing together the 55 countries of the African Union (AU) and eight (8) Regional Economic Communities (RECs). See more information and the text of the Agreement at the official website <https://www.afronomicslaw.org/category/analysis/digital-trade-african-continental-free-trade-agreement-exploring-its-promises-and>. [↑](#footnote-ref-5)
6. Emmanuel Salami, "Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection Law in Africa" 66 *Journal of African Law* 2 (2022), <https://www.cambridge.org/core/journals/journal-of-african-law/article/implementing-the-afcfta-agreement-a-case-for-the-harmonization-of-data-protection-law-in-africa/29DD231B417FFA84110030B9D03A2005>. [↑](#footnote-ref-6)
7. See Ayalew, *op.cit*. [↑](#footnote-ref-7)
8. All data available at the database of UNCTAD, Cybercrime Legislation Worldwide, available at <https://unctad.org/page/cybercrime-legislation-worldwide> and at the Global Cybersecurity Index of ITU, available at <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>. [↑](#footnote-ref-8)
9. See article 23, paragraph 2 of the Constitutive Act of the AU, adopted on 11 July 2000. The full text is available at the official website of the AU at <https://au.int/en/constitutive-act>. [↑](#footnote-ref-9)
10. See Orji, *op. cit.* [↑](#footnote-ref-10)
11. See the report by African Union and Symantec Corporation, *Cyber Crime & Cyber Security Trends in Africa* (November 2016), <https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf>. [↑](#footnote-ref-11)
12. CETS No. 108, available at <https://www.coe.int/en/web/data-protection/convention108-and-protocol>. [↑](#footnote-ref-12)
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [↑](#footnote-ref-13)
14. Alex B. Makulilo, "The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius" 25 *The International Journal of Human Rights* 1 (2021), <https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1783532?src=recsys>. [↑](#footnote-ref-14)
15. Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2019). [↑](#footnote-ref-15)
16. Article 32 of the AU Convention. [↑](#footnote-ref-16)
17. Mohamed Aly Bouke, Sameer Hamoud Alshatebi, Azizol Abdullah, Korhan Cengiz, Hayate El Atigh, "African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions", arXiv:2307.01966 (5 July 2023), <https://doi.org/10.48550/arXiv.2307.01966>. [↑](#footnote-ref-17)