WUJL, Nov-Dec.2024,2(1), 56-71)
DOI: https://doi.org/10.20372/wujl.v2i1.1336
ISSN: 2226-7522 (Print) and 3005-7612 (Online)
Wallaga University Journal of Law
WUJL, November- December. 2024, 2(1), 56-71
Home Page: https://journals.wgu.edu.et

Original Article

Globalization of Computer Networks: The Need for Accession to Regional Cybercrime Treaties

**Obsa Degabasa Abaje*

*****Obsa Degabasa is a Senior Lecturer in Law at Wollega University School of Law, an independent consultant, and a lawyer at any of the Federal Courts of Ethiopia and the Oromia Regional State Courts. The author is a member of the Ethiopian Federal Bar Association and the Oromia Lawyers' Association. He can be reached at: obsadegabasa@gmail.com/ obsad@wollegauniversity.edu.et/ +251-917097109.

Abstract

Cross-border communication and data sharing are now more feasible than ever due to the globalization of computer networks. Criminals exploit this connection, making the criminal justice system more vulnerable. The Federal Democratic Republic of Ethiopia is aware of the national security challenges that have been exposed while integrated into the global information network. To do this, a lot of work is indispensable to build capacity and implement international best practices, robust policy, and an effective legal framework. Ethiopia adopted the Information Security Policy in 2011, with the legal objective of preventing, deterring, responding to, and prosecuting acts of crime against information and information infrastructure, and protecting the confidentiality, availability, integrity, and authenticity of information. Most of the principles in the policy were incorporated in Computer Crime Proclamation No.958/2016. The Proclamation criminalizes different offenses on a computer or a computer system with new legal mechanisms and procedures to prevent, control, investigate, and prosecute computer crimes and facilitate the collection of electronic evidence. However, the legitimacy of criminal justice authorities to secure electronic evidence is argumentative, as it is not subject to any conditions or safeguards for human rights as rule of law safeguards. Then the purpose of the paper is to provide a comprehensive understanding of Ethiopian cybercrime, highlighting the benefits of harmonizing national law with other cybercrime treaties to combat cybercrime effectively.

Article Information

Article History:
Received: 4-8-2024
Revised: 22-10-2024
Accepted: 9-11-2024

Keywords:
Cybercrime,
Criminal Justice,
Legitimacy,
Computer Networks

***Corresponding Author:**
Obsa Degabasa
E-mail:
obsadegabasa@gmail.com

1. Introduction

Numerous academic works have attempted to define computer crime. However, there is no single clear definition of the word. The challenge of cybercrime starts with the lack of a clear definition. Although there is no singular legal definition for the term, more common or general references are used, such as cybercrimes, electronic communications, information and communication technologies, or high-tech crime. In addition, international and regional legal instruments are not defined with clarity and specificity due to the term's complexity, multiplicity, and universal nature.

For instance, the Council of Europe Cybercrime Convention, which is the first international treaty on crimes committed via the Internet and other computer networks, deals with lists of acts,[1] (for instance, confidentiality, availability, integrity, infringements of copyright, computer-related fraud, child pornography…) and other crimes rather than providing the meaning for the term. This Convention serves as a guide for the member states to develop comprehensive national legislation against cybercrime and as a framework for international cooperation between state parties to this treaty.[2] Not only for member states or invited to the Budapest Cybercrime Convention but also beyond the Signatories, the convention serves as a guide or at least as a source inspiring domestic legislation for many countries,[3] this also includes Ethiopia.[4] This Budapest Convention is supplemented by Protocol No. 189 on xenophobia and racism committed through computer systems.[5] The convention currently complemented again the second additional protocol on enhanced cooperation and disclosure of electronic evidence.[6] The Protocol and the draft Protocol simply supplement the Budapest Convention with a few additional features of cybercrimes. The African Union Convention on Cyber Security and Personal Data Protection does not provide a clear definition of the term but simply identifies a list of acts that could constitute cybercrime.[7]

Ethiopia's Computer Crime Proclamation No. 958/2016 is legislated to provide authorities with legal mechanisms and procedures to prevent, control, investigate, and prosecute computer crimes and facilitate the collection of electronic evidence in Ethiopia. Article 2 of this proclamation defines computer crime as a crime committed against a computer, computer system, computer data, or computer network. Not only these, but also a conventional crime

[1] Council of European on Cybercrime Convention, (European Treaty Series - No. 185, 2001) (hereafter, BC),Art.211, availableat:https://www.refworld.org/docid/47fdfb202.html [accessed 20 January 2024]

[2] Ibid., Preamble, Par 1

[3] The global state of cybercrime legislation 2013-2021: A cursory overview, The technical report prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC) under the projects GLACY+,Cyber East, I proceeds 2, Cyber South and Octopus Project 30 June 2021

[4] See Computer Crime Proclamation No.958/2016 the substantive criminal law part from Art 3- 7 used Budapest Convention on cybercrime 2001, from Art 2-6 as guideline for each provision.

[5] Council of Europe, Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, 28 January 2003 availableat:https://www.refworld.org/docid/47fdfb20f.html [accessed 25 February 2024]

[6] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, opened for signature by the States Parties to Budapest Convention on Cybercrime (Treaty ETS 185) on 12/05/2022

[7] African Union Convention on Cyber Security and Personal Data Protection, 2014, (hereafter, AUC) Art 29 & 30.

committed utilizing a computer, computer system, computer data, or computer network, and Illegal computer content data disseminated through a computer, computer system, or computer network can be taken as computer crime by this proclamation.

Currently, several countries, including the global South, have made progress in the development of ICT infrastructure as a process of digitalization. This progress in the development of information and communication technologies (ICTs) drives economic and social developments to achieve sustainable development goals (SDGs).[8] For developing countries, including Ethiopia, sustainable development (Agenda) includes ICT goals and is expected to be the driving factor for economic and social development. However, there are still dark sides to these revolutions in ICT, and cybercrime is the dominant one. This creates the use of ICT in unexpected ways and ways in 2030 that aggravate critical infrastructure and other individual rights.[9] This makes the criminal justice response to cybercrime too complicated.[10] Furthermore, combating cybercrime through the criminal justice system in the global south, especially in Ethiopia, seems to be the residual work of the government, while security responses are the primary role of the government authorized to protect national security.

The responses of the state to cybercrime could be through legal regulatory measures or non-legal regulatory means.[11] Here, nonlegal regulatory responses are most of the time institutional responses towards hybrid cyber threats and cyber-attacks. In most cases, it is a technical response to critical public infrastructure, such as power grids, financial institutions, aviation authorities, and utilities.[12] This could be handled by INSA in Ethiopian cases, as it is authorized as a cyber command institution in this country.[13] These nonlegal regulatory measures could be taken most of the time through Internet shutdown, and web filtering, and these could be all about cyber security concerns. On the other hand, fighting cybercrime through a legal regulatory response is about governing cybercrime issues by law, and it could be done through the formal justice system. Different types of policies and laws govern Security threats, and it could be done through applying these laws. In Ethiopia, these laws are FDRE's Constitution, [14]National Information Security Policy,[15] Computer Crime,[16] hate speech and disinformation prevention and suppression law,[17] Electronic

[8] Faturoti, Bukola, Internet Access as a Human Right and the Justiciability Question in the Post-COVID-19 World (2024) 15 (1) European Journal of Law and Technology.

[9] Obsa Degabasa [2024]. Cybercrime Threats and Trends in Ethiopia: A Critical Legal Analysis. Wallaga University Journal of Law, 1(2), p 22.

[10] Ibid

[11]International Law series, volume IV Addis Ababa University –School of Law, ISSN:2708-1745, The Internet and Policy Responses in Ethiopia New Beginnings and Uncertainties

[12] Ibid

[14] [The]e Federal Democratic Republic of Ethiopian Information Network Security Agency Re-establishment Proclamation No. 808/2013 Art 5

[14]Constitution of the Federal Democratic Republic of Ethiopia Proclamation No. 1/1995 available at: https://www.refworld.org/docid/3ae6b5a84.html [accessed march 2024]

[15] National Information Security Policy of the Federal Democratic Republic of Ethiopia September 2011

[16] The Federal Democratic Republic of Ethiopian Computer Crime Proclamation No. 958/2016 (hereafter, ECC)

[17] The Federal Democratic Republic of Ethiopian Hate Speech and Disinformation Prevention and Suppression Proclamation No.1185 /2020

Signature Proclamation,[18] INSA Re-establishment Proclamation No. 808/2013,[19] Personal Data Protection Proclamation No.1321/2024,[20]…etc. However, the focus of this article is on the computer crime law of 958/2016.

Computer-related crimes are on the rise in the 21st century due to the proliferation of computers, their integration into all human activities, and the Internet being the environment that dominates communication.[21] As a result, the criminal justice system, in general, and criminal law, in particular, face legal challenges. These problems are different from ordinary crimes in that cybercrimes are technology-related crimes that cannot be properly handled by regular criminal justice institutions. As a result, the criminal justice system will expect to be adequate,[22] to impose punishment on criminals and protect against damage to people, data systems, computer, computer systems, computer networks, and other critical infrastructure. In doing this, it is expected that criminal law will be strong and adequate in criminalizing acts, defending individual rights, facilitating international cooperation to aid in the collection of electronic evidence, and enabling the investigation and prosecution of a crime using fundamental rules of evidence and criminal procedure. However, this is complicated by other factors that countries cannot address alone. This is due to the difficulties that law enforcement agencies face when dealing with cross-border legal issues and data access issues. This required countries to participate in the harmonization process of cybercrime laws, allowing countries to effectively combat cybercrimes.

2. Global and Regional Initiatives

These initiatives emphasize the relevance of both binding and nonbinding agreements in the worldwide battle against cybercrime, and the investigation relies on certain dominant legal documents. There are different initiatives in reaction to cyber-crime attacks; Some nations have approved national laws and others have agreed to follow some regional legal instruments that have been adopted.[23] The UNODC is developing a comprehensive international treaty to combat the use of information and communication technologies for illegal purposes. This requires multistakeholder participation, including civil society and academics. Interpol's effort, on the other hand, aims to strengthen the ability of law enforcement organizations around the world to combat cybercrime through training, operational support, and information exchange.[24]

---

[18] The Federal Democratic Republic of Ethiopian Electronic Signature Proclamation No.1072/2018

[19] The Federal Democratic Republic of Ethiopian Information Network Security Agency Re-establishment Proclamation No. 808/2013

[20] The Federal Democratic Republic of Ethiopian Personal Data Protection Proclamation No.1321/2024

[21] Cited at note 11.

[22] Black's Law Dictionary defines "adequate" as sufficient, commensurate, equally efficient, equal to what is required, suitable to the case or occasion, satisfactory…etc. The American Heritage College Dictionary defines "adequate" as sufficient to meet a need. The operational definition that the researcher intended to use for the term adequacy is the Criminological Concept of Adequacy (sufficient to prevent, control, investigate, and prosecute the suspects of Cybercrime or computer crimes and facilitate the collection of electronic evidence) in Ethiopian criminal justice system as indicated at the preamble 4th paragraph of The Federal Democratic Republic of Ethiopian Computer Crime Proclamation No. 958/2016.

[23] https://www.unodc.org/unodc/en/ngos/harnessing-global-responses-to-a-new-un-cybercrime-convention.html Last accessed on December 4, 2024

[24] Ibid

2.1 Global Perspective of the Budapest Convention (for all countries)

The Budapest Convention on Cybercrime, commonly known as the Council of Europe Convention on Cybercrime, is the oldest and most important regional initiative combating cybercrime. It was made available for signing in Budapest, Hungary, on November 23, 2001, and went into effect on July 1, 2004. This agreement is the first international pact aimed at combating cybercrime by standardizing national laws, strengthening investigative procedures, and increasing international cooperation.[25] The Convention has had a global impact on cybercrime legislation, and several nations outside of Europe have embraced it as well. It establishes a comprehensive framework for countries to participate in the fight against cybercrime, making it a cornerstone of global efforts to address this growing threat. The Convention established pillars to guide its vision and implementation. Domestic Criminal Law Harmonization: The goal is to unify the legal provisions of the signatory states on offenses involving the confidentiality, integrity, and availability of computer data and systems. [26]The convention establishes certain procedural powers for the collection of electronic evidence. Establishes procedures for rapid international cooperation, which is frequently required given the transnational character of cybercrime. The Convention also addresses the issue of protecting rights and liberties while guaranteeing cyber security.[27]

2.2 Budapest Convention and Ethiopian Computer Crime Law 958/*2016*

The analysis will be the Budapest Convention on Cybercrime and The Ethiopian Computer Crime Proclamation No.958/2016. The Budapest Convention provides a framework for international collaboration between State Parties to this convention and guidelines for creating comprehensive national laws against cybercrime. The convention specifies rules for procedural processes (investigative and prosecution methods), international legal support (such as extradition or cross-border access to digital evidence), and substantive laws (minimum standards for what is criminalized). This legal framework provides cybercrime legislation that is expected to serve at least three purposes.28 These are first the criminalization of conduct ranging from illegal access to systems interference, computer-related fraud, child pornography, and other content-related offenses. Second, there are procedural law tools to investigate cybercrime and secure electronic evidence concerning any crime,[29] and the third is efficient international cooperation.[30]

These three legal purposes will be helpful to see the framework and effectiveness of

[25] Cited at note 3
[26] Ibid
[27] Ibid
[28] Cited at note 23, p.23, The content of Budapest convention on cybercrime framework embodies Criminalization of the act, Procedural laws and the International cooperations. These components work together to create a comprehensive legal framework for combating cybercrime on a global scale.
[29] See Art 14 to 21 of the Budapest convention, which provides a set of procedural tools for law enforcement, such as the search and seizure of computer data, real-time collection of traffic data, and interception of content data.
[30] See Art 23 to 35 of the Budapest convention, which establishes a framework for international cooperation, including mutual legal assistance, extradition, and the establishment of a 24/7 network to facilitate immediate assistance in cybercrime investigations.

Ethiopia's computer crime law.[31] These might be crimes committed against or via computers. The categories include substantive criminal law, such as offenses against confidentiality, integrity, availability of computer data, and systems. Computer-related crimes, such as fraud and forgery, are among the ranges of offenses criminalized under the first function.[32] Criminalization also includes content-related offenses.[33] This also includes issues of the human rights of an individual, the right to privacy,[34] freedom of expression,[35] and other human rights that are recognized under different international and regional human rights instruments.[36] When it comes to these international instruments, a balance is needed between combating cybercrime and upholding human rights. Adequate cybercrime legislation is necessary to control cybercrime, and legitimate legal procedures and mechanisms are expected. To be effective, these are expected from Ethiopian laws. Certain human rights are legally prohibited in certain situations (although some rights may not be curtailed owing to international human rights legislation. These restrictions are authorized when they are in pursuit of a legitimate aim, by existing law, and necessary and proportionate to the threat that justified their implementation.[37] The concrete range of legitimate goals depends on the applicable human right and may include the interests of public safety, national security, and protection of the rights of others.[38] In addition to the need for the restriction to serve one of the legitimate aims mentioned above, the restriction must be based on national law. This law must be accessible to citizens to enable them to regulate their behavior and reasonably foresee the powers of authorities in the enforcement of this law and the consequences of non-compliance. It must be precise and avoid providing State authorities with unbounded discretion to apply limitations.[39] Vague and overbroad justifications, such as unspecific references to national security, extremism, or terrorism, do not qualify as adequately clear laws. Necessary means that the restriction must be something more than useful, reasonable, or desirable. Moreover, there must be an appropriate relationship between the legitimate aim pursued by a state and the actions of the state to achieve that legitimate aim. In other words, the actions must be proportionate to the interest to be protected. This implies that the restriction is the least intrusive instrument among those which might achieve the desired result. States have some latitude in the way they fulfill their obligations under international human rights law.

The procedural rules that give criminal justice authorities the ability to obtain electronic

[31] Look at the preamble of the Proclamation no 958/2016(The fourth paragraph……. it has become necessary to incorporate new legal mechanisms and procedures in order to prevent, control, investigate and prosecute computer crimes and facilitate the collection of electronic evidence is standard of adequacy to combat cybercrime in Ethiopian context)

[32] See BC. Art (2 to 11) and ECC. Art (3 to 6).

[33] See BC. Art 9 and ECC. Art (12 to 14).

[34] Universal Declaration of Human Rights (hereafter, UDHR) Article 12., International Covenant on Civil and Political Rights 1966 (hereafter, ICCPR). Article 17., The European Convention on Human Rights of 1950, (hereafter, ECHR) Article 8, and The American Convention on Human Rights of 1969. (hereafter, ACHR) Article 11

[35] UDHR. Art 19., ICCPR. Art 19., ECHR Art 10, ACHR Art 13 and Article 9(2) of the African Charter on Human and Peoples' Rights of 1981. (hereafter, ACHPR)

[36] Ibid

[37] Ibid

[38] Ibid

[39] see Human Rights Committee, General Comment No. 34 ,2011

evidence related to cybercrime are the second primary objective of cybercrime legislation.[40] Determining the crime committed and by whom is the purpose of criminal justice, in general, and the legislation on criminal procedure, in particular.[41] Criminal justice is focused on ensuring the criminal process, as well as the capture and punishment of perpetrators (investigation and prosecution). [42]The criminal procedure serves two purposes in this regard. This could serve as one way to implement substantive criminal law and another way to distribute power among those involved in criminal justice (police, prosecutor, judge, victim, and defense lawyer).[43] The exact value anticipated in a fair criminal justice [44]is related to outcomes such as reliable conviction of the guilty and exoneration of the innocent. This function is a collection of specific procedural rules that specify in detail the authority that the law enforcement organ may exercise when looking into a crime committed against or using computers set up under the first function. As a safeguard for the rule of law, these procedural powers must be subject to restrictions and protections for individual rights.[45] However, these restrictions and protections for individual rights in Ethiopian computer crime law are argumentative as there are no safeguards.

The third function of cybercrime legislation is almost the extension of the second function to the international arena, providing a mechanism for international cooperation in matters not only related to cybercrime but also police-to-police and judicial cooperation to any crime involving electronic evidence.[46] Global connectivity[47] and the ICT revolution have resulted in globalization in computer networks or internet penetration of the Internet even at the African level while increasing and increasingly easy to use, ensuring its availability to both criminals and victims. Criminals use this as an opportunity and use it for their culpable purposes. As a result, collecting electronic evidence has become a global issue that requires collaboration between nations. Harmonized national substantive cybercrime laws that punish cybercriminals and national procedural laws that establish the standards of evidence and criminal procedure are essential for international cooperation. By harmonizing bilateral, regional, and multilateral cybercrime instruments as needed, international cooperation can also be made easier. Legal compliance with regional and multinational cybercrime instruments also requires their ratification or accession.

[40] See BC. Art (14 to 15) and ECC. Art (29 to 38)

[41] See Wondwossen Demissie, Ethiopian Criminal Procedure A textbook (School of Law, Addis Ababa University, (2012).

[42] Ibid

[43] Ibid

[44] The term “fair criminal justice process” is to indicate criminal procedure conducted fairly, justly, and with procedural regularity by an impartial judge and in which the defendant is afforded his or her rights under the Federal Constitution or state constitution or other law. Among the factors used to determine fairness is the effectiveness of the assistance of counsel, the opportunity to present evidence and witnesses, the opportunity to rebut the opposition's evidence and cross-examine the opposition's witnesses, the presence of an impartial judge, and the judge's freedom from bias.

[45] See BC. Art 15

[46] See BC. Art (23 to 24). and ECC. Art 42.

[47] The term “global connectivity” refers the ability of the internet to provide the possibility of seamless communication throughout the whole planet. This has a wide range of advantages. Individually, it makes possible for those who relocate or travel to stay in touch with friends and relatives all around the world.

Concerning the Budapest Convention on cybercrime, signatories must act on a national level to combat cybercrime, including modifications and additions to substantive legislation and criminal procedure law (to establish the procedures for criminal investigations and prosecutions). The Convention further provides signatories with guidance on mutual assistance and acts as a mutual legal assistance treaty (i.e., an agreement between countries to cooperate on investigations and prosecutions of certain or all offenses proscribed by both parties under national law). Regarding international cooperation under the Council of European Conventions, Parties shall cooperate through the application of relevant international instruments on international cooperation in criminal matters.[48] The agreement is based on uniform or mutual legislation and domestic laws, to the widest extent possible, for investigations or proceedings concerning criminal offenses related to computer systems and data or for the collection of evidence in the electronic form of a criminal offense.

The adoption of appropriate legislation against cybercrime for criminals or activities designed to affect the integrity of critical infrastructures at the national level is important.

This requires coordinated action related to prevention and response by the government through legal instruments (legal-regulatory response). Establishing legal sanctions for cybercriminals and preventing harm to people, data systems, services, and infrastructure is expected to be robust. Such a law is also expected to be helpful in protecting individual rights, enable investigation and prosecution of a crime committed online, and facilitate cooperation between/among/ cybercrime matters of different jurisdictions.

However, several technical reasons make cybercrime difficult to combat. One is the attribution in the investigation of cybercrime. The investigation is difficult because any computer connected to the Internet can communicate with any other multiple computers on the Internet. This is what makes the globalization of computer networks. Cybercrime inevitably often has an extraterritorial aspect that can give rise to complex jurisdictional issues that involve people present and acts that are being carried out in many different countries. In addition, the investigation of computer crimes and the gathering of appropriate evidence for criminal prosecution can be an extremely difficult and complex issue, due primarily to the intangible and often transient nature of data, especially in a network environment. Technology renders the investigation and recording process of evidence extremely vulnerable to defense claims of errors, technical malfunction, prejudicial interference, or fabrication. Such claims may even lead to a ruling from the court against the admissibility of such evidence.

Having these difficulties in hand, legal measures play a key role in the prevention and combating of cybercrime, especially legal challenges. These are required in all areas, including criminalization, procedural powers, jurisdiction, international cooperation, and the responsibility and liability of the Internet service provider. While doing this, the use of criminalization and criminal law calls for respect for human rights such as freedom of

[48] See BC. Art.23.

expression,[49] privacy,[50]and other constitutional rights that must be respected. Concerning these international instruments, such as the International Covenant on Civil and Political Rights, put it as everyone shall have the right to freedom of expression,[51] similarly, the FDRE Constitution incorporates the right to freedom of expression as everyone has the right without any interference.[52] Regarding the right to privacy, the FDRE Constitution clearly stipulates that everyone has the right to privacy, and this right shall include the right not to be subjected to searches of his home, person, or property, or the seizure of any property in his possession.[53] Similarly, UDHR has boldly given attention to the right of privacy, as no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, or to attacks upon his honor and reputation. And everyone has the right to the protection of the law against such interference or attacks.

Thus, currently, the administration of criminal justice including both terrestrial and virtual justice needs adequate and legitimate policy and legal frameworks. In digital societies,[54] cybercrime is frightening and can represent an almost endless list of different criminal justice concerns that may arise from technical to legal challenges and solutions ranging from technical to legal that require a policy and legal response through the harmonization of dominant cybercrime treaties.[55]

2.3 The significant benefits of the Budapest Convention on Cybercrime Globally

The convention establishes a legal framework for mutual legal aid, which facilitates cross-border investigations and prosecutions.[56] Furthermore, the treaty establishes clear extradition rules, which serve to ensure that cybercriminals are brought to justice regardless of where they are located.[57] The Second Additional Protocol to the Budapest Convention on Cybercrime concerns greater international cooperation in cybercrime and electronic evidence. This protocol is intended to increase the efficiency and effectiveness of international cooperation among the convention's parties. The convention harmonizescybercrime definitions, minimizing legal disparities and enabling a uniform strategy for combating cybercrime.

[49] Cited at note 16. Art. 29

[50] Ibid. Art. 26.

[51] ICCPR). Art. 19(2).

[52]Cited at note Art 29(2)

[53] Ibid, Art 26/2

[54] The notions of" digital society" reflects the results of the modern society in adopting and integrating information and communication technologies at home, work, education and recreation, and as the result digital innovations are reshaping our society, economy and industries with a scale and speed like never before.

[55] Common challenges in combating cybercrime as identified by Eurojust and Europol June 2019 (Since the Court's rulings, the lack of unified retention of electronic communication data across the EU has proven a key challenge to investigating cross-border cybercrime. The operational experiences of both agencies have shown that technically collection of electronic communication data is the key to the successful investigation and prosecution of serious crimes, including cybercrime……. Comprehensive analyses performed by Eurojust and Europol Data Protection Function after the 2014 CJEU ruling, have underlined the value of electronic communication data for criminal investigations and prosecutions and have shown that most of the law enforcement and judicial authorities support a legislative framework at the EU level.)

[56] The Budapest Convention on Cybercrime addresses mutual legal assistance in Article 25. This article outlines the procedures and requirements for countries to provide mutual legal assistance to each other in the investigation and prosecution of cybercrimes.

[57] The Budapest Convention on Cybercrime provides extradition in Article 24. This article indicates the procedures and requirements for extradition for cybercrime offenses covered by the convention.

The convention contains materials for training law enforcement and judicial agencies, which will improve their ability to investigate and prosecute cybercrimes.[58] This technical aid helps to build the infrastructure required to effectively combat cybercrime. The Budapest Convention on Cybercrime promotes human rights through its provisions.[59] Specifically, Art. 15 focuses on the safeguarding of human rights and liberties. It ensures that the measures adopted to prevent cybercrime are balanced with the need to protect fundamental human rights such as privacy and freedom of expression.[60] The treaty incorporates measures to preserve human rights and to prohibit the abuse of cybercrime legislation for political gain.

Measures to counteract cybercrime shall be implemented in a way that protects people's privacy. The convention also covers a wide range of cybercrimes, ensuring a variety of cyber dangers.

By aligning its legislation with the Budapest Convention, Ethiopia can strengthen its legal and institutional framework, increase international cooperation, and improve its overall cybersecurity posture. This will help protect citizens and companies from the growing threat of cybercrime.

2.4.Malabo Convention (African perspective)

The African Union Convention on Cybersecurity and Personal Data Protection, often known as the Malabo Convention, is regarded as one of the most significant regional initiatives since the Budapest Convention. It was adopted on 27 June 2014 and intends to build a legislative framework for cybersecurity and data protection in African countries.[61] This project demonstrates the growing realization of the need for comprehensive cybersecurity measures and the cooperation of African governments to effectively combat cybercrime.[62]

The Malabo Convention on Cyber Security and Personal Data Protection entered into effect on June 8, 2023, a decade after being adopted on June 27, 2014. This milestone was achieved on 9 May 2023, when Mauritania ratified the convention, making it the 15th ratification required for it to become effective.[63]

The Malabo Convention is currently the only legally binding regional data protection convention outside of Europe, establishing a comprehensive framework for cybersecurity, personal data protection, and electronic commerce in Africa. It aims to streamline data protection legislation, increase digital rights,

[58] The Budapest Convention emphasizes the importance of capacity building and training in various sections, particularly in the context of international cooperation and procedural measures. The Cybercrime Convention Committee (T-CY) and the Cybercrime Program Office of the Council of Europe (C-PROC) play significant roles in providing training and technical assistance to member states to enhance their capabilities in combating cybercrime.

[59] International Human Rights Instruments Standards is expected as minimum protection under the convention. Article 15 aligns with international human rights instruments, such as the European Convention on Human Rights and the International Covenant on Civil and Political Rights, reinforcing the commitment to protecting human rights in the digital age. By incorporating these principles, Article 15 ensures that the fight against cybercrime does not come at the expense of fundamental human rights, including the right to privacy.

[60] Ibid

[61] Cited note at 9

[62] Ibid

[63] The Malabo convention officially enter into force June 8,2023 , https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281 Last accessed on December 1, 2024

and strengthen cybersecurity measures in African Union member states.[64]

2.5 The significant benefits of the Malabo Convention for African countries

The Malabo Convention establishes a comprehensive framework for cybersecurity, strengthening national cybersecurity measures, and protecting critical infrastructure. The Malabo Convention on Cyber Security and Personal Data Protection covers better cybersecurity in multiple provisions, with Article 25 explicitly focusing on cybersecurity measures. This article describes the member state's responsibility to implement legal, technical, and organizational measures to safeguard the security of electronic communications and key information infrastructure. The agreement stresses the protection of personal data, requiring worldwide standards for data privacy and security.65 Ratification of the Malabo Convention would increase collaboration with other African countries in combating cybercrime and protecting personal data.[66] Art 29 of the Malabo Convention on Cyber Security and Personal Data Protection outlines member states' obligations to promote and enhance capacity building in the field of cybersecurity and personal data protection, emphasizing the significance of training. Capacity building can help member states develop the skills and expertise required to effectively address cyber threats. It emphasizes the importance of training, education, and awareness-raising activities to strengthen individuals' and institutions' capabilities in combating cyber threats and protecting personal data.

3. The Budapest Convention on Cybercrime Vs. Malabo Convention on Cyber Security and Personal Data Protection

The Budapest Convention on Cybercrime establishes a comprehensive framework for combating cybercrime and protecting electronic evidence.67 Its framework and primary objectives include, but are not limited to, the following. Criminalization of cybercrime defines various cybercrimes, including illegal access, data interference, system interference, and computer-related fraud.68 It sets procedures for law enforcement, such as computer data search and seizure, faster data preservation, and real-time traffic data collection. 69 The convention facilitates international cooperation in

[64] The AU took important action on cybersecurity at its 2024 summit, https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed accessed on December 2, 2024

[65] The Malabo Convention on Cyber Security and Personal Data Protection addresses data protection in Article 8, in which this article provides the obligations of member states to introduce a specific national legal framework for the protection of personal data, aimed at safeguarding fundamental rights such as freedom of expression and the right to privacy.

[66] The Malabo Convention on Cyber Security and Personal Data Protection addresses regional cooperation in Article 28, in which the article gives the obligations of member states to cooperate at the regional level to enhance cybersecurity and protect personal data. It emphasizes the importance of collaboration among African Union member states to effectively combat cyber threats and ensure the security of electronic communications.

[67] BC Art 1 Provides the purpose of the convention, which is to pursue a common criminal policy aimed at the protection of society against cybercrime, through the adoption of appropriate legislation and fostering international cooperation.

[68] Cited note at 27

[69] BC art 19. outlines the procedures and requirements for the search and seizure of computer data, ensuring that law enforcement agencies have the necessary tools to investigate and prosecute cybercrimes effectively.

cybercrime investigations, including mutual legal assistance, extradition, and the establishment of a 24/7 network for immediate assistance.70 The convention aims to harmonize national laws, improve investigative techniques, and increase cooperation among nations to effectively combat cybercrime.71 The Budapest Convention on Cybercrime has a broad scope of applicability, addressing various aspects of cybercrime and electronic evidence. These include Illegal Access: Unauthorized access to computer systems and networks. Data Interference: Unauthorized alteration, deletion, or suppression of computer data. System interference: Disruption of the functioning of computer systems. Misuse of devices: Possession and distribution of devices or software designed for the commitment of cybercrimes. Computer-Related Fraud: Fraudulent activities involving computer systems. Child Pornography: Offences related to the production, distribution, and possession of child pornography. The convention protects human rights and liberties. [72]This convention can be considered purely a digital criminal justice treaty. The Budapest Convention on Cybercrime is a global treaty. Although originally adopted by the Council of Europe, it is open to all countries around the world. This global applicability enables a complete and coordinated international response to combating cybercrime and securing electronic evidence. Budapest Convention on Cybercrime includes additional themes beyond the core provisions. These themes are addressed through their additional protocols. First Additional Protocol (Racism and Xenophobia) This protocol criminalizes acts of a racist and xenophobic nature committed through computer systems. It aims to combat hate speech and related offenses online. Second Additional Protocol (Enhanced International Cooperation) This protocol focuses on enhancing international cooperation and the disclosure of electronic evidence. It provides additional tools and measures to facilitate cross-border investigations and improve the efficiency of mutual legal assistance. These additional protocols expand the scope of the Budapest Convention, addressing specific issues, and enhancing the overall framework for combating cybercrime and securing electronic evidence. Implementing the Budapest Convention is a continuous process that involves regular evaluations, updates to national laws, and ongoing international collaboration to address emerging cyber threats.

The Malabo Convention, officially known as the African Union Convention on Cyber Security and Personal Data Protection, is a comprehensive framework designed to improve cybersecurity, protect personal data, and promote electronic commerce in Africa. The African Union adopted the convention on 27 June 2014, in Malabo, Equatorial Guinea. The convention sets out principles and guidelines for the protection of personal data,[73]

[70] See BC Art 35. Speaks the creation of a network of contact points available 24 hours a day, 7 days a week, to provide immediate assistance in cybercrime investigations and facilitate international cooperation.

[71] See BC Art 2. It indicates the need for member states to adopt legislative measures to criminalize certain activities related to cybercrime, ensuring a consistent legal framework across different jurisdictions.

[72] See BC Art 15 It Ensures that measures taken to combat cybercrime shall be balanced with the need to protect fundamental human rights, such as the right to privacy and freedom of expression.

[73] See AUC Art 11 Data Protection Authority's Mandates the establishment of a national data protection authority (DPA) with administrative independence to monitor and enforce data protection laws, Art 13

ensuring individuals' privacy rights are safeguarded. It advocates initiatives to improve cybersecurity in member states by addressing digital threats and vulnerabilities.[74]

The convention establishes guidelines for secure electronic transactions, thus increasing trust and confidence in digital commerce.[75] The convention contains under Chapter One issues related to electronic commerce, under Chapter Two personal data protection, and Chapter Three issues related to cybersecurity and cybercrime. This indicates that the Malabo convention is not purely a criminal justice convention; rather, it can be considered as general information technology law including non-criminal justice issues. The convention specifically targets African Union member states, encouraging them to adopt and implement its provisions to create a harmonized legal framework throughout the continent.

4. Conclusions and Recommendations

The Ethiopian government has paid attention to creating the legal and legislative framework required to combat the widespread use of cybercrime. To preserve confidentiality, availability, integrity, and authenticity of information. Ethiopia has adopted the Information Security Polic while its legislative purpose is to prevent, deter, respond to, and prosecute acts of crime against information and information infrastructure. The Computer Crime Proclamation No. 958/2016 is the official translation of the policy. The law has made several deeds illegal as a means of preventing and combating cybercrime. The Ethiopian Computer Crime Proclamation No. 958/2016 is a relatively recent addition to the body of law that makes a variety of acts illegal as cybercrime. Various unique evidence and procedural rules have also been introduced, which will help with the investigation and prosecution of cybercrimes. The Proclamation is rife with a host of issues, such as illegal access to a computer,[76] illegal interception, interference with a computer system, causing damage to computer data,[77] as a crime against computer systems and computer data, and as computer-related crimes such as computer-related fraud, electronic theft, and combating child pornography.[78]

However, the development of new international legal instruments is an opportunity to strengthen international cooperation mechanisms and obtain extraterritorial evidence in practice and to build the capacity of law enforcement and criminal justice institutions.[79] This maintains the inadequacy caused by the lack of jurisdiction in cybercrime offenses. In this regard,

Provides the core principles governing the processing of personal data, such as consent, lawfulness, confidentiality, and transparency and Art 16 to 19 Confers various rights on individuals concerning the protection of their personal data, including the right to access, rectify, and delete their data. These articles collectively provide a comprehensive framework for personal data protection within the Malabo Convention.

[74] See AUC Art 24. This article mandates that every member state develop a national cybersecurity policy and strategy. In addition to that Art 26 to 28 outline the establishment of various institutions and procedures to identify and respond to cybersecurity incidents, promote cybersecurity principles, and ensure international cooperation.

[75] See AUC Art 2 to 8 These articles outline the legal framework for secure electronic transactions, promoting trust and confidence in digital commerce within the African continent.

[76] ECC., Art 3

[77] Id, Art 4-6

[78] Id, Art 9-12

[79] BC. Art 23.

criminalization of acts, harmonization,[80] of domestic laws with international and regional laws, accession to existing international or regional cybercrime instruments and application of existing law determine whether the law is adequate,[81] to govern the issue.[82]

Everyone can see that The Ethiopian Computer Crime Proclamation No. 958/2016 has drawn the law from the Budapest Convention on Cybercrime except for the conditions and safeguards for human rights. It is possible to review one by one. For instance, in the case of substantive criminal law part ECC Art 3, as Illegal Access Criminalizes unauthorized access to computer systems. Under the Budapest convention, Art 2 defines illegal access to computer systems. Similarly, data interference, unauthorized alteration, deletion, or suppression of computer data are criminalized under Art 4 of BC and Art 4 of ECC without any difference. With regards to system interference, ECC Art. 5 Criminalizes actions that disrupt the functioning of computer systems, and similarly BC Art. 5 defines system interference as the intentional hindering of the functioning of a computer system. Criminalization regarding misuse of computer devices and data. ECC Art. 7 addresses the possession and distribution of devices or software designed for committing cybercrimes, while BC Art. 6 criminalizes the misuse of devices, including the production, sale, and distribution of tools intended for committing cybercrimes. Definitions of terminology are also similar, for instance, what traffic data explained under BC Art 1(d) is the same as with ECC Art 2(6). Similarly, computer-related forgery was criminalized under ECC Art 9, whereas the BC criminalized it under Art 7. Computer-related fraud issues are criminalized under ECC Art 10, while under BC Art 8. Under these provisions almost all elements for the criminalization of an act are the same that establish crime, for instance, the act should be without authorization, excess in authorization, and intentionally or non-public computers without the right to do so. On the other hand, content-related offenses like child pornography were criminalized in both Budapest convention under Art 9 and under Ethiopian computer crime law under Art 12 with no difference.

Regarding procedural measures, The Ethiopian Computer Crime Proclamation 958/2016 adopted what was the Budapest Convention including provisions for the search and seizure of computer data, preservation of data, and real-time collection of traffic data. The difference between the two here is that The Ethiopian Computer Crime Proclamation no.958/2016 has not adopted what is mentioned under Art. 15 of Budapest convention conditions and safeguards during search and seizure for criminal justice authorities. These conditions and safeguards during the investigation are a guarantee of human rights protection and maintain due process of law. On the other hand, criminal law by itself is the highest government interference

[80] The context of "harmonization" is both in terms of substantive and Procedural provisions (harmonization of substantive provisions of cybercrime law helps facilitate international cooperation (prevents cybercrime safe havens,) and harmonization of procedural provisions of cybercrime laws facilitates, among other things, global evidence collection and sharing through international cooperation.

[81] Cited at note 22

[82] It also contains a series of powers and procedures such as the search of computer networks and lawful interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering.

in the freedom and liberty of an individual. Conducting a search and seizure of this digital ecosystem of an industry without conditions and safeguards will be an exception. In addition to that, the purpose of a fair and reliable criminal justice system is to maintain the conviction of guilt and exoneration of innocent, this will be more achieved if regional and global cooperation is done to do so.

The Ethiopian Computer Crime Proclamation 958/2016 Art. 42 Emphasizes the need for international cooperation in combating cybercrime. While Budapest Convention Art. 23 to 35 Establish a comprehensive framework for international cooperation, including mutual legal assistance, extradition, and a 24/7 network for immediate assistance. The Ethiopian Computer Crime Proclamation has indeed adopted several principles and provisions from the Budapest Convention to combat cybercrime. However, as the country has not yet ratified, the benefits of international cooperation that the convention holds were not utilized. Currently, more than 69 countries have ratified the Budapest Convention on Cybercrime, including those outside of Europe. For Ethiopia international cooperation is almost all about bilateral agreement rather than treaty-based one. But ratifying the Treaty makes Ethiopia more beneficial, at least for now it can allow cooperating with 69 countries around the world. This, on the other hand, advances international cooperation to fight cybercrime.

Regarding the conditions and safeguards during the investigation, what was adopted by the Budapest Convention on Cybercrime is up to the standard for human rights protection, which is also the state commitment. The lack of these conditions and safeguards for Ethiopian computer crime 958/2016 attracted criticism that the country is expected to do so. It should be in line with international human rights instruments. Again, in line with this, Ethiopia will benefit if she ratifies it. In addition to that, training for packages of the Budapest convention on cybercrime is something valuable for Ethiopians in which skilled manpower will be realized to invest gate and prosecute the cybercrime. One of the big problems to invest in and prosecute cybercrime is the lack of skilled manpower.

Currently, Ethiopia has not yet ratified the Malabo Convention on Cyber Security and Personal Data Protection. While the convention has entered into force, many African Union member states, including Ethiopia, have not yet completed the ratification process.

Ratification of the Malabo Convention is critical for harmonizing cybersecurity and data protection regulations across Africa, increasing cooperation, and improving the overall cybersecurity posture of the continent. The convention aims to harmonize data protection and cybersecurity laws in Africa, facilitating cooperation and coordination between member states. It enhanced Security by promoting robust cybersecurity measures, the convention helps protect critical information infrastructure and reduce cyber threats. The convention provides a legal framework for electronic commerce, which can help Ethiopia develop its digital economy and promote e-commerce. In general, the Malabo Convention represents a significant step toward strengthening cybersecurity, protecting personal data, and promoting digital commerce in Africa. The convention promotes regional cooperation in the combat of cybercrime, enabling Ethiopia to work more effectively with other African countries to address transnational cyber threats. Ethiopia introduced a law on personal data

protection in here jurisdiction, which is called Federal Democratic Republic of Ethiopian Personal Data Protection Proclamation No.1321/2024. However, ratification helps to align Ethiopia's data protection standards with international norms and ensure robust protection of personal data, even in cross-border contexts. By adhering to the Malabo Convention, Ethiopia can benefit from improved international cooperation in data protection, including sharing best practices, technical assistance, and support in addressing cross-border data protection challenges.

Regarding information sharing ratification, the convention facilitates better information sharing and collaboration with other countries, improving the overall effectiveness of cybersecurity, cybercrime prevention, and response efforts.

Regarding encouraging consistency in regulations, the Malabo Convention urges member states to adopt consistent cybersecurity and data protection laws. This harmonization of legal frameworks supports the AfCFTA's objective of creating a unified market by reducing regulatory barriers and ensuring a level playing field for businesses. It also promotes economic development through enabling digital economic growth. Both the Malabo Convention and the AfCFTA contribute to the growth of the digital economy in Africa. By providing a secure environment for digital transactions and protecting personal data, the Malabo Convention supports the AfCFTA's efforts to boost intra-African trade and economic development. The Malabo Convention and the AfCFTA are complementary initiatives that together improve the digital and economic landscape of Africa. By promoting cybersecurity, data protection, and secure digital transactions, the Malabo Convention supports the AfCFTA's goal of creating a robust and integrated African market.

It also increases investor confidence. The Malabo Convention creates a more secure, predictable, and investor-friendly environment, which can attract both domestic and foreign investments. A robust legal framework for cybersecurity and data protection can increase investor confidence, attracting more investment in Ethiopia's digital sector.

So, by adhering to the Malabo Convention, Ethiopia can strengthen its legal and institutional framework, improve cybersecurity measures, protect personal data, and improve international cooperation, contributing to a safer and more secure digital environment. The Directive also establishes foreign currency saving accounts (FCY) for various entities and individuals, opens the securities market to foreign investors, and permits industry parks and Special Economic Zones to engage in transactions. Overall, these changes aim to liberalize and streamline foreign exchange transactions and regulations in Ethiopia. Looking at their contents and the amount of modifications they have made to the previous forex regime, these new regulations do have far-reaching repercussions on FDI in Ethiopia. Yet the practical effects of the new law on FDI are yet to be seen.

.