DOI: https://doi.org/10.20372/wujl.v1i2.1074
ISSN: 2226-7522 (Print) and 3005-7612 (Online)
Wallaga University Journal of Law
WUJL, March- April. 2024, 1(2), 18-33
Home Page: https://journals.wgu.edu.et

Original Article

Cybercrime Threats and Trends in Ethiopia: Critical Legal Analysis

Obsa D.*

Obsa Degabasa *is a Lecturer -in -Law at Wallaga 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. The writer can be reached at: obsadegabasa@gmail.com/ obsad@wollegauniversity.edu.et/ +251-917097109*

Abstract

Computer technology and computer-related issues are a recent phenomenon in world history. This phenomenon is even relatively recent in Ethiopia. Hence, computer-based and computer-generated crimes and the resultant laws and enforcement have never been closely examined particularly in Ethiopia. Accordingly, Ethiopia has recently been tackling computer crimes in proclamations and regulations. It has lately implemented legislative measures in response to the growing availability and adoption of information and communication technologies. On June 7, 2016, Ethiopia's House of People's Representatives legislated the Computer Crime Proclamation. The proclamation addresses several issues, including unauthorized computer access, to combating terrorism and as well as child pornography. To prevent, control, investigate, and prosecute computer crimes and gather electronic evidence, a new set of legal mechanisms and procedures were incorporated into the Proclamation. This paper's primary goal is to investigate the adequacy of legislation and enforcement mechanisms of computer crimes under the Ethiopian legal system in line with regional and international covenants. The analysis's primary focus is on examining the strengths and limitations of the substantive and procedural laws, digital evidence, and evidentiary rules. The paper critically explores the prevailing legal and practical challenges concerning computer crime laws in Ethiopia. Finally, the paper includes important recommendations for improving substantive and procedural aspects of criminal justice about computer crimes in Ethiopia.

Article Information

Article History:
Received: 14-11-2023
Revised: 25-02-2024
Accepted: 11-03-2024

Keywords:
Computer crime, Cybercrime, Internet law, Substantive laws, Procedural laws

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

1. Introduction

Alvin Toffler divides global history into three distinct waves: the agricultural, industrial, and information eras.[1] We are currently experiencing the third wave of information technology worldwide.[2] However, technology is neutral and can empower both destructive and constructive individuals. Like any new invention, technology will always have its supporters who see only positive effects and its detractors who see only negative effects. Criminals have always utilized opportunities in new technologies. A large number of people fall victim to cybercrime every day and suffer trillions of dollars in financial and property loss worldwide.[3] Even defining the terms complex and variant technological terms of cybercrimes is not an easy task.[4] Numerous research studies have demonstrated that the term cybercrime encompasses a wide range of newly emerging forms of abuse and criminality made possible by information and communication technologies (ICT). The terms "computer crime," "cybercrime," "high-tech crime," "e-crime," and "electronic crime" are commonly employed synonymously to refer to two primary categories of offenses, i.e. cybercrime, computer, or computer-related crimes. Computer crimes are a relatively new phenomenon in the modern world and are expanding at a rapid pace. However, the working definition for cybercrime or computer crime for this paper is any unlawful conduct focused using electronic actions that targets the security of computer systems and the data processed by them.

Nowadays Information and Communication Technology Systems (ICTS) are embraced in all facets of life. The introduction, growth, and utilization of information and communication technologies have been accompanied by increasing and sophisticated criminal activities. Cybercrimes have increasingly become a major and serious concern for the global community. They are international and transnational crimes that have been induced by the global revolution in ICTS, and the new forms of computer crimes present new challenges to lawmakers, law enforcement agencies, and international institutions. This necessitates the existence of effective legal mechanisms that monitor and prevent the utilization of ICTS for criminal activities in cyberspace.

Cyber-crimes can be more harmful than traditional once, since cyber offenders can deploy multi-pronged attacks and innovate at any time, from anywhere, partly or completely anonymously, against information systems. The magnitude and speed of cybercrime require proactive and cautionary measures as they will affect the security and economic interests of the nation. During the enforcement of computer crime in Ethiopia, it is expected that different strategies will be implemented and directives will be issued following the legislation of computer crime law.[5]

The computer crime law of the Federal Democratic Republic of Ethiopia has been drafted and adopted as one of Ethiopia's

[1] *Asmare, Mollalign. "Computer crimes in Ethiopia: An Appraisal of the legal frame work" International Journal of Science and Humanities Research, Volum 3, Issue 1 Page 93 March 2015.*

[2] *Richard power tangle web tales of digital crimes from the shadow of cyberspace (QUE corporation U.S.A 2000 P.4)*

[3] *Halefom Hailu, The state cybercrime governance in Ethiopia, (May 2015,) p. 7*

[4] *McQuade 2011,2or legal and political measures to address cybercrime by Matheus M. Hoscheidt.*

[5] *The Federal Democratic Republic of Ethiopian Computer Crime Proclamation No. 958/2016 (hereafter, ECC) Art 44*

criminal laws as of June 7, 2016. The main objectives of the computer crime legislation of 2016 are to protect Ethiopia's economic and political stability.[6] The proclamation explains that Ethiopia's existing legal framework is not adequately tuned with the technology changes and is insufficient to prevent, control, investigate, and prosecute the suspects of computer crime.[7] The Ethiopian government is constructing ICT infrastructures and ICT-based services, which will eventually lead to a greater dependence on these infrastructures and services.[8] However, it is a fact that with reliance on computer systems and other digital technologies comes vulnerability to cybercrime and cyber-attack as a result of connection to global cyberspace.[9] Therefore, Ethiopia is open to cybercriminals operating anywhere in cyberspace right away as it connects to a global network. Thus, the threat to Ethiopia is indeed real, not imaginary.[10]

Enforcing a computer crime law that is, accessible, predictable, and efficient while adhering to the rule of law is essential to promoting good governance, democratization, and economic growth, as well as maintaining public safety and peace.

The purpose of this paper is, therefore, to critically examine the main substantive and procedural aspects of the computer crime laws of Ethiopia and its practice starting from its legislation in terms of its legal content and procedure. The focus of the analysis is on examining the strengths and limitations of the substantive and procedural laws, digital evidence, and evidentiary rules. It further explores the computer crime law of Ethiopia and its implementation given the legal standards of the existing national, regional, and international computer crime laws.

2. The Context of Computer Crime in Ethiopia

The internet was first made available in Ethiopia in 1997, but access was restricted.[11] As KinfeYilma said Ethiopia is currently amongst the countries with the lowest level of Internet penetration and use. As a result, some argue that internet-related crimes are not imminent threats to Ethiopia.[12] However, Kinfe asserts that since the adoption of the computer crimes laws, several cybercrimes have been committed against Ethiopian cyberspace.[13] There are hundreds of cybercrimes in this country every year that go undetected by the government.[14] He acknowledges that there aren't many documented court cases, though.[15]

On the other hand, some believe that the Ethiopian government is wary of the detrimental effects of the internet on its authority.[16] The government allegedly fears that the use of the new technology or the internet unsettles the existing power structure. As a result, the neglect of providing reliable and affordable internet connections in the major towns, including the capital, is attributed

[6] *Ibid . Pre-Amble Paragraph one.*
[7] *Article 19, Ethiopian computer crime proclamation July 2016 legal analysis page 5 paragraph one*
[8] *Ibid*
[9] *Ibid*
10Halefom Hailu, cyber law and policy researcher at INSA, The state of cybercrime governance in Ethiopia
[11] *Kinfe Micheal Yilma, Ethiopia's new cybercrime legislation: Some reflections, computer law & security review 33 (2017) 250–255, P 252*
[12] *Ibid*
[13] *Halefom Hailu Abraha and KinfeMichealYilma."The Internet and Regulatory Responses in Ethiopia." Mizan Law Review, (September 2015), Vol. 9, No.1. p. 112*
[14] *Ibid*
[15] *Ibid*
[16] *Ibid*

to such fear. There is only one Internet Service Provider, Ethio Telecom, which is owned and operated by the Ethiopian state.[17]

The Ethiopian government has faced pressure to liberalize the telecommunications sector, particularly from the West. A few members of civil society also criticize the situation on the ground, claiming that the public monopoly and lack of competition are to blame for the underperformance of the Ethiopian telecommunications industry.

However, the Ethiopian government has a long history of maintaining its firm position that it will not liberalize the telecom industry anytime soon until recent time. This is primarily because the telecom industry provides the majority of the funding for large-scale projects like the construction of telecommunications infrastructure in rural areas with high costs, such as the railway. Currently, though, there is some indication that the government is willing to allow the partly privatization process to begin in the telecommunications industry. This partly privatization process manifested in agreement with the new telecom provider, Safaricom Ethiopia.

Government institutions are dealing with the regulation of cyberspace in Ethiopia. While they have different objectives, ranging from cyber security, online video, and web advertising, all of them have the legal authority to regulate online content. Given that there is some doubt about these overlapping competencies, how does content regulation operate? The current regulatory framework in Ethiopia is sector-specific due to the fact that broadcasting and telecommunications are governed by different agencies and have disparate legal frameworks. We can now days use the internet to share music, watch television, and make phone calls from handheld devices like smartphones, blurring the lines between the once distinct sectors of broadcasting, ICT, and telecom.

This digital convergence poses challenges to existing governance functions as it makes regulatory overlapping inevitable. Additionally, it casts doubt on regulations about new services made possible by digital technologies like the Internet. Thus, research suggests that another difficulty faced by Ethiopian regulators is the overlap in power and the inactivity of regulatory responsibilities. Even though the issue of internet freedom and national security is not only an Ethiopian problem she faces a great problem. At the moment, it is the subject of a heated international discussion. Finding the ideal balance between internet freedom and other justifiable interests like national security and law enforcement is the largest challenge facing all governments today. As a young democracy, these challenges are more pressing in Ethiopia. On the one hand, the government has legitimate national security and law enforcement interests that cannot be ignored. However, the government must uphold the rights that are stipulated in the constitution, such as the freedom of the internet. This is a demanding position that calls for a strong legal and regulatory framework that guarantees a sufficient degree of protection while also advancing Ethiopia's interests in public security and law enforcement.[18]

International human rights organizations denounce the Ethiopian government for

[17] *Ibid*

[18] *The issue of internet freedom and national security is not only an Ethiopian problem (see Halefome Hailu and Till Waescher)k8*

establishing a political environment that puts peace and development ahead of enabling a diversity of voices to compete in the marketplace of ideas. Additionally, it is charged with suppressing oppositional viewpoints, including those of civil society organizations, which bemoan the fact that serious transgressions and human rights breaches have been ignored in the sake of nonviolent progress that could be advantageous to the nation.[19]

The fact that protecting national, military, foreign policy and international relations is a good thing, believes that such a measure should not violate individuals' freedoms and rights. However, points out that considering the small number of internet users and the limited chances of cyber-attacks, the introduced measures are disproportionate. The penalty and punishment regime in the computer crime law of the revised criminal code of 2004 and the computer crime law of 2016 does not take the country's specific situation into account. On the one hand, cybercrime by its nature requires preparation, intent, and knowledge. On the other hand, the literacy rate and internet access in Ethiopia is extremely low. In this context, the penalty does not give meaning. It includes overly excessive punishments including ill-defined aggravated cases of cyber criminality[20]

1.1. The Adequacy of Ethiopian Law in line with the Budapest Convention.

The criminality involving computers is on the rise in the 21st century due to the proliferation of computers, and their integration into every part of human activities as well as the internet being the environment dominating any communication.[21] The criminal justice system, in general, and criminal law, in particular, faces legal challenges as a result.[22] These problems are distinct from ordinary crimes in that cybercrimes are technology-related crimes that cannot be properly handled by regular criminal justice institutions. As a result, it is expected that the criminal justice system will be adequate,[23] to impose punishment on criminals and guard against damage to persons, data systems, computers, computer systems, computer networks, and other critical infrastructure. While doing this, it is expected that criminal law will be strong and adequate in the criminalization of acts, in defending individual rights, facilitating international cooperation to aid in the collection of electronic evidence, and enabling the investigation and prosecution of a crime through the use of fundamental rules of evidence and criminal procedure.

The Budapest Convention on Cybercrime, which serves as a guideline for developing comprehensive national legislation against

[19] *Ibid*

[20] *Is cyberattack is an imminent threat to Ethiopia? Knife M/ Yilma p 36*

[21] *A conversation on the Future of Cyber Security on Oct 11, 2017, at UN University of Tokyo Center for Policy Research Director (Sabastian Von Einsiedel) with Melissa Hathaway, who served as a senior cyber security adviser to both Presidents George W. Bush and Barack Obama and leading a major Cyberspace Policy Review for the latter.*

[22] *Ibid*

[23] *Black's Law Dictionary defines "adequate" as sufficient, commensurate, and 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 Concepts 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.*

cybercrime and a framework for international cooperation between State Parties to this treaty (see Chapter III) will be used as a standard for the comparative study. The Convention includes requirements for substantive laws (minimum standards for what is criminalized) procedural mechanisms (investigative and prosecution methods) and international legal assistance (such as cross-border access to digital evidence or extradition). This legal framework provides cybercrime legislation expected to serve at least three purposes.[24] These are first the criminalization of conduct ranging from illegal access to systems interference, computer-related fraud child pornography, and other content-related offences. Second, are procedural law tools to investigate cybercrime and secure electronic evidence concerning any crime, and the third is efficient international cooperation.

These three legalpurposes will be used to eval uate how well Ethiopia's computer crime law's function.[25] These could be offenses against and using computers. The categories include substantive criminal law, like offenses against confidentiality, integrity, and availability of computer data and systems as computer-related crimes such as fraud and forgery are among the ranges of offenses criminalized under the first function.[26] The criminalization also includes content-related offenses.[27] Oftentimes, online content is connected to basic principles rule of law. This includes issues of constitutional rights of an individual, in particular, the right to privacy,[28] and freedom of expression.[29]

The second purpose of the cybercrime legislation is procedural laws which provide criminal justice authorities procedural powers to secure electronic evidence not only concerning cybercrime but also in any other crime.[30] Determining the crime committed and by whom is the purpose of criminal justice, in general, and criminal procedure legislation, in particular.[31] Criminal justice is focused on ensuring the criminal Process as well as the capture and punishment of perpetrators (Investigation and prosecution). 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).[32] The exact value anticipated in a fair criminal justice, [33]is related to outcomes such as dependable conviction of

---

[24] *The Budapest Convention on Cybercrime: benefits and impact in practice, Cybercrime Convention Committee(T-CY), Strasbourg, on 13 July 2020, " https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac" Last visited on September 28/2022*

[25] *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 evidences is standard of adequacy to combat cybercrime in Ethiopian context).*

[26] *Council of European on Cybercrime Convention, (European Treaty Series - No. 185, 2001) (hereafter, BC) Art (2-11) and ECC. Art (3-6).*

[27] *BC. Art 9 and ECC. Art (12-14).*

[28] *Universal Declaration of Human Rights (hereafter, UDHR) Article 12. and International Covenant on Civil and Political Rights 1966 (hereafter, ICCPR) .Article 17.*

[29] *UDHR. Article 19. and ICCPR . Article 19.*

[30] *BC. Art (14-15) and ECC. Art (29-38)*

[31] *Wondwossen Demissie, Ethiopian Criminal Procedure A text book (School of Law, Addis Ababa University,(2012).*

[32] *Ibid*

[33] *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*

the guilty and exoneration of the innocent. This function is a collection of specific procedural rules that specify in great detail the authority that law enforcement organs 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.[34]

Herbert L. Packer, a legal professor, developed two models for criminal justice regarding procedural powers, which criminal justice authorities play.[35] These models are referred to as Crime Control and Due Process. The criminal justice system in Packer, especially when attempting to hold offenders accountable for their wrongdoings, may be rather complex. The public expects the system to be competent, swift, and effective while upholding each person's rights and administering justice fairly. Once these objectives have been balanced, justice will be served if crime is reduced, offenders are punished promptly, and individual constitutional rights are respected.[36] The Crime Control Model contends that to overcome the conflict, the law's enforcement objective of criminal proceedings should take precedence over the fairness goal. The Due Process Model, on the other hand, prioritizes the fairness of the trial over the goal of upholding the law. Although neither model is realistic, they do represent the two extremes of the range of potential approaches to delivering justice.[37] These models do not directly represent any particular criminal justice system including Ethiopian, but they do highlight aspects of those systems that correspond to certain objectives and ideals as conceptual framework. Both approaches set general guidelines to combat crime and penalize those who perpetrate it.

According to the due process paradigm, every person should have access to a reasonable and equitable criminal justice system that respects their constitutional rights. According to this concept, a citizen has rights and cannot be denied their rights like the right to life, liberty, or property without following the correct legal procedures and safety protections. The crime control model, in contrast, was said to highlight the importance of effectively suppressing criminal activity in the interest of maintaining public order. It entails quick, unofficial, and routine processes that are handled by criminal justice professionals. This model emphasizes having an effective system, with the primary goal being to suppress and control crime to maintain public order and safety in society. According to this theory, protecting individual freedom comes second to reducing crime. This model represents a more traditional viewpoint of government's role. The crime control model would support swift and severe punishment for offenders to safeguard society and ensure that people are free from the threat of crime.

According to this model, the legal system can resemble an assembly line where prosecutors charge suspects, law enforcement officers apprehend them, the courts declare guilt, and then convicted individuals are given suitable and severe punishments through the criminal

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.

[34] *BC. Art 15.*

[35] *Herbert L.Packer "Two Models of the Criminal Process,"113 University of Pennsylvania Law Review 1(1964) (hereafter Packer, "Two Models")*

[36] *Ibid.*

[37] *Cited at note 36*

justice system.[38] According to the principles of the crime control model, for instance, the failure of law enforcement to firmly regulate criminal activity is seen as causing the collapse of public order, which eventually results in the absence of a crucial element of human freedom. The Crime Control Model mandates that the effectiveness,[39] with which the criminal process functions to screen suspects, decide guilt, and gain suitable dispositions for those convicted of a crime be given significant focus to achieve this reasonable goal. The Crime Control Model's high purpose calls on the criminal procedure to screen suspects effectively, assess guilt, and secure adequate punishments for those found guilty.

People are notoriously bad observers of disturbing events, and the more emotionally charged the context; the more likely it is that recollection will be inaccurate. Confessions and admissions by people in police custody may be induced by physical or psychological coercion so that the police end up hearing what the suspect says. Due Process Values reject this evidence in favor of a view of informal, non-adjudicative fact-finding that emphasizes the possibility of error. All of these factors lead to the rejection of informal fact-finding procedures as being conclusive of factual guilt and the persistence of formal, adjudicative, adversarial fact-finding procedures, where the factual case against the accused is heard in public by an impartial tribunal and is evaluated only after the accused has had a full opportunity to refute the case against him. This Model places a strong emphasis on preventing and getting rid of errors as much as possible. Therefore, it is not necessary to make widespread, illegal practices legal. Instead, it is to reiterate their illegality while also taking action to diminish their occurrence. This paradigm of due process places legitimacy at the center. Although the models prioritize opposing criminal justice ideologies, it is still conceivable to discuss how this conceptual framework might be used to evaluate the adequacy and legitimacy of a particular criminal justice system.

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.[40] Global connectivity[41] and the ICT revolution have resulted in globalization in computer networks, and the technology is universal and increasingly easy to use, ensuring its availability to both criminals and victims. Criminals use this as an opportunity and utilize it for their guilty purposes. As a result, gathering electronic evidence becomes a global issue that necessitates collaboration between nations. Harmonized national substantive cybercrime laws that punish cybercriminals and national procedural laws that establish the norms 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

[38] *Packer, Two Models .P.10.*

[39] *The term "effectiveness" means here the system's capacity to catch, try, convict, and dispose of at least high proportion of criminal offenders whose offenses become known.*

[40] *BC. Art (23 -24). and ECC.Art 42.*

[41] *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.*

easier. Legal compliance with regional and multinational cybercrime instruments also requires their ratification or accession.

Concerning the Budapest Convention on Cybercrime, signatories must take action 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 co-operation under the Council of European Convention puts, the Parties shall cooperate with each other through the application of relevant international instruments on international cooperation in criminal matters.[42] 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 intended 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 law is also expected to be helpful in protecting individual rights, enabling investigation and prosecution of a crime committed online, and facilitating cooperation between/among/ cybercrime matters of different jurisdictions.

However, several technical reasons make fighting cybercrime difficult. One is attribution on cybercrime investigation. The investigation is difficult because any computer that is 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 to it that can give rise to complex jurisdictional issues that involve persons present and acts 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 networked environment. The technology renders the process of investigation and recording 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 for the legal challenges. These are required in all areas, including criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability. While doing this the use of criminalization and criminal law calls for

[42] *BC. Art.23.*

respect of the constitutional rights of an individual as freedom of expression,[43] privacy,[44] and other constitutional rights that should be respected. Concerning these international instruments like International Covenant on Civil and Political Rights put it every one shall have the right to freedom of expression,[45] and similarly, the FDRE Constitution incorporates the right to freedom of expression as everyone has the right without any interference.[46] Regarding the right to privacy, the FDRE Constitution 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 under his/her possession.[47]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 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 equally needs adequate and legitimate policy and legal frameworks. For digital societies,[48] cybercrime is frightening and can stand for an almost endless list of different criminal justice concerns that may arise from technical to legal challenges and solutions ranging from technical to legal which call upon policy and legal response by legislation.[49]

Attention has been paid by the Ethiopian government to creating the required legal and legislative framework to combat the widespread use of cybercrime. To preserve the confidentiality, availability, integrity, and authenticity of the information, Ethiopia has adopted the Information Security Policy of 2011, 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 law's official translation of the policy. The law has made several behaviors 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. Several 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, like illegal access to a computer,[50] illegal interception, interference with a computer system, causing damage to computer data,[51]

[43]*Constitution of the Federal Democratic Republic of Ethiopia Proclamation No. 1/1995(hereafter FDRE constitution), Art. 29*

[44] *Ibid .Art 26*

[45] *ICCPR). Art.19 (2)*

[46]*Cited at note 44, Art 29(2)*

[47] *Ibid, Art 26/2*

[48] *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.*

[49]*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 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 the majority of law enforcement and judicial authorities support a legislative framework at EU level.)*

[50] *ECC., Art 3*

[51] *Ibid., Art 4-6*

crime against computer systems and Computer data, and also as computer-related crimes like Computer-related Forgery, computer-related fraud, electronic theft and combating child pornography.[52]

2. Infringement to Human Rights and Fundamental Freedoms

There are advantages and disadvantages to the law. In terms of content substantively, the 2016 proclamation is thorough and up to date. A number of recently developed cybercrimes are now included in the existing laws by the Computer Crime Law. In particular, it covers the admissibility of electronic evidence, the production and preservation of electronic data, and the search and seizure of computer data. It also introduces comprehensive procedural and evidentiary rules that are essential in the investigation and prosecution of computer crimes. On the other hand, the 2016 computer crime law violates citizens' fundamental constitutional rights and freedoms, including their right to privacy, their freedom of speech, and the due process of law. This runs counter to the administration's claim that Ethiopia is a democratic nation.[53]

It may be contended that the most troublesome part of the 2016 computer crime law is concerning the warrantless digital forensic investigation that it authorizes INSA to conduct. Where there are reasonable grounds to believe that computer crimes are likely to be committed, INSA investigators can conduct without any judicial oversight virtual forensic investigation into computers suspected to be sources of attack or to be subjected to attacks. When compared with other developing countries, what makes our laws unique is that it shows our attitude to court warrants. However, this law restricts the role of the court. The court has no involvement whatsoever in the most crucial investigation processes. The INSA people can conduct the forensic investigation virtually without presenting at your office and physically touching your computer but without court authorization is unprecedented elsewhere including the Budapest Convention. It should also be noted in this connection that physical examination requires a court warrant. Moreover, about this, INSA investigators are also allowed to carry out, again, warrantless sudden searches against suspected computers for preventive purposes.

Additionally, the law imposed a one-year minimum data retention requirement on communication service providers for data passing through their networks. This requirement is an obvious legislative overreach that makes it possible for rights to data privacy to be violated. The issue is that the law's mandated data retention period is very long, and it could be difficult to maintain the data of many clients for an extended period of time. A concerning clause in the law concerns communication service providers and is related to the recently added "duty to report" provision. When service providers learn of cybercrimes being committed or the distribution of illicit content, such as child pornography, via their computer systems, they are obligated to notify the INSA and the police. The issue with such a requirement is that it might force service providers to proactively monitor communication on their networks in order to avoid the severe consequences that the law foresees for their refusal to assist law enforcement. Even worse, because of this technically demanding legal requirement, service providers would have to use algorithmic bots to automatically identify

[52] *Ibid., Art 9-12*

[53] *Cited at note 12*

illegal activity, which could violate users' right to free speech online as well as their right to privacy. It's similar to keeping an eye on your compound to make sure no crimes are being committed there. Additionally, the cybercrime law contains provisions that contradict fundamental procedural justice tenets like due process of law. The law, for instance, allows courts to rule ex parte on a request by investigators for a production order against a person thought to have computer data needed for investigation.[54] They are giving a production order even without the presence of the person concerned, who could have legitimate reasons to protest an otherwise unreasonable request erodes due process rights. Another important principle of procedural justice abrogated by the law relates to the burden of proof in cybercrime proceedings.[55] The law states that where the Prosecutor has proved 'basic facts', the court may on its motion shift the burden of proof to the accused.[56] This proviso violates a long-established principle of criminal justice which levies on the government the burden to prove guilt beyond any reasonable shadow of doubt and the constitutional principle which requires the accuser to prove the guilt of the accused. Among the issues offered in this paper, understanding what is meant by Computer Crime, in the international context must be followed Ethiopian issues. Ethiopia has been enacting various pieces of legislation to regulate some aspects of the digital environment. The Cybercrime Proclamation of 2016 is a new law that makes a number of cybercrimes illegal. Additionally, it has brought in a number of cutting-edge procedural and evidentiary guidelines that will support the investigation and prosecution of cybercrimes. However, it attracts censures from substantive and procedural corners mainly owing to some of its human rights, privacy rights, and due process rights. The cybercrime legislation incorporates provisions that present a potential threat to the right to privacy and principles of procedural justice. The right to privacy is guaranteed under FDRE Constitution Article 26,[57] and international treaties,[58] like the International Covenant on Civil and Political Rights to which Ethiopia is a state party. The legislation contained concerning clauses that could infringe upon these rights protected by the constitution. One such provision allowed INSA to carry out digital forensic investigations on computers believed to be involved in cyber-attacks, without the need for a court-issued warrant, if there was sufficient evidence to suggest that computer crimes were imminent.[59] Additionally, it empowered INSA investigators to conduct warrantless sudden searches against suspected computers for preventive purposes. Following a flurry of criticism against these rules, the law has mandated a prior judicial warrant before such far-reaching measures are taken by INSA.[60] INSA, however, still wields the power to conduct warrantless virtual not physical digital forensic investigations under its reestablishment proclamation of 2013.[61] Recent subordinate legislation that furthers the 2013 reestablishment proclamation has intriguingly included the requirement of a judicial warrant to conduct a forensic

[54] *ECC Art 31/2*
[55] *ECC Art 37/2*
[56] *Ibid*
[57] *FDRE Constitution Art 26*
[58] *ICCPR Art 17*
[59] *ECC Art 32/2*
[60] *Ibid*
[61] *Information Network Security Agency Re-establishment Proclamation, Federal Negarit Gazeta, Proclamation No. 808/2013, Art 6(8).*

investigation by INSA.[62] The pertinent sections of the Regulation state that the Agency is required to conduct a digital forensic investigation in collaboration with pertinent investigative entities as per Article 6(8) of the INSA Reestablishment Proclamation and under the authority of a court. The discrepancy between these two laws is quite perplexing and not easily understood, considering that regulations are considered secondary legislation within Ethiopia's legal framework. This implies that the proclamation takes precedence in cases of contradiction, yet the intention to address any shortcomings of the proclamation through subordinate legislation raises questions as to why.

It is crucial to emphasize the necessity of judicial oversight for the proclamation. The lack of any oversight mechanism by the courts is what makes the power of sudden searches and virtual forensic investigations so concerning for privacy rights. The power granted for sudden searches under the law could be significantly more invasive, especially when compared to other Ethiopian laws that outline similar search processes.

Another worrying provision of the law relates to the newly inserted duty to report obligations on communication service providers, and government organs.[63] INSA is additionally mandated to establish, through a Directive, the specific format and process for conducting the reporting. Service providers have an obligation to promptly notify INSA and the Police upon discovering instances of cybercrimes or the dissemination of illicit material, such as child pornography, on their computer systems. The apprehension surrounding this requirement is that it may compel service providers to proactively monitor communications on their networks, as failure to cooperate could result in penalties. Nevertheless, the consequences for service providers failing to fulfill their reporting duty remain uncertain. The additional cause for alarm is that the law allows for a single judicial warrant to be used to investigate multiple computer systems. This provision raises the possibility of accessing data stored in computer systems that are linked to the system covered by the warrant. While this provision is based on the Council of Europe and African Union Cybercrime Conventions, it raises valid concerns. Specifically, the broad nature of the warrant undermines the rights of individuals whose computer systems may be accessed without their knowledge. Allowing extension of virtual or physical search warrants initially granted to a specific computer system to another system appears.

The legislation on cybercrime also encompasses regulations that undermine fundamental principles of procedural justice, such as the right to due process. For example, the law permits courts to make unilateral decisions on a request by investigators for a production order against an individual believed to possess computer data relevant to an investigation. Issuing a production order without the presence of the affected person, who may have valid concerns, undermines the rights to due process. Moreover, the disclosure of personal computer data during the enforcement of such an order also raises concerns regarding data privacy rights. Additionally, the law appears to disregard another crucial principle of procedural justice,

[62] *Council of Ministers Regulation to Provide for Execution of Information Network Security Agency Reestablishment Proclamation, Federal Negarit Gazeta, Regulation No. 320/2014, Art 10(1).*

[63] ECC Art 27/1

which pertains to the burden of proof in cybercrime proceedings. The law states that where the Prosecutor has proved basic facts, the court may, on its motion, shift the burden of proof to the accused.[64] This provision contradicts a well-established principle of criminal justice that places the responsibility of proving guilt beyond a reasonable doubt on the government. Furthermore, it undermines the presumption of innocence for the accused, as the mere decision to shift the burden suggests that the prosecutor has already established a strong case. Considering the limited experience in cybercrime investigation and prosecution in Ethiopia, there is also a concern that prosecutors may rely on this provision even when there is insufficient evidence against the suspects. In cases involving complex technicalities, a prosecutor may request the court to alter the burden of proof by presenting somewhat inconclusive evidence, such as the presence of a person's face in illicit content or involvement in criminal activities unrelated to the suspect. This situation is more probable when innocent individuals' computers are compromised and manipulated by hackers to carry out cybercrimes like DoS attacks. As a result, regular individuals who are suspected of committing cybercrimes will face significant challenges in disproving the presumption of evidence once the burden has been shifted.

3. Conclusions

Term definitions are frequently found in particular legislative acts. But term definitions aren't always well-defined by legislators. Occasionally, they do not define at all, leaving law enforcement to make educated guesses until the courts rule. The extremely wide definition of Ethiopian computer crime is one of the main criticisms levelled at it. There is no precise definition of computer crime or distinction between cybercrime and computer crime in Ethiopia. Thus, it ought to be as explicit as other laws, and there ought to be a distinction made between cybercrime, computer crime, and computer-related crimes. To say there is cybercrime three things should exist. These are Computer, network, and internet, whereas in the Ethiopian context there are no differences in terminologies.

In 2011, the government developed a policy and in 2016, passed legislation on cybercrime. By enacting Computer Crime Proclamation No. 958/2016, she has taken legal action to combat cybercrime. The law's purpose is to provide appropriate protection and security measures for the use of information communication technology, which is susceptible to a variety of computer crimes and other security threats that could jeopardize individual rights and impede the nation's overall development. [65] By this law, the country has criminalized different offenses against and using computers citing that the existing laws were not adequately tuned with the technological changes and are not sufficient to prevent, control, investigate and prosecute the suspects of computer crimes.[66] As a result, it has become necessary to incorporate new legal mechanisms and procedures to prevent, control, investigate, and prosecute computer crimes and facilitate the collection of electronic evidence adequately.[67]

On the other hand, the development of new international legal instruments is an opportunity to strengthen mechanisms for international cooperation and obtaining extraterritorial evidence in practice and

64 ECC Art 37/2
65 ECC Pre-amble, par 2.
66 ECC , Pre-amble, par 3
67 ECC., Pre-amble, par 4

capacity building for law enforcement and criminal justice institutions.[68] This maintains the inadequacy caused by a lack of jurisdiction in cybercrime offenses. In this regard, the criminalization of the acts, harmonization,[69] of domestic laws with international and regional laws, accession to existing international or regional cybercrime instruments, and application of the existing law determine whether the law is adequate,[70] to govern the issue.[71]

According to government statements,[72] official INSA reports, and other research, computer crime offenses in Ethiopia have increased since the passage of the Computer Crime Law. On one hand, the critique is not only inadequacy of the law to govern the offense but also the legitimacy about criminal justice authorities, in procedural powers to secure electronic evidence. As to the Packer's Dues process criminal justice model (as formal fact-finding process), having a just and fair criminal justice system for all and a system that does not infringe upon the constitutional rights of an individual is what means by due process. This model is the type of justice system that is based on the principle that a citizen has rights and cannot be deprived of their rights like right to privacy,[73] and freedom of expression,[74] without appropriate safeguards. This model reviews whether the law contains safeguards against arbitrariness is the focus. The philosophical background of the Due Process model is the preservation of the constitutional rights of individuals and the protection of human rights. Under Ethiopian computer crime law, procedural powers to secure electronic evidence are with no safeguards.[75] To protect individual rights still Ethiopia relies on general procedural law provisions for search, and seizure to collect evidence. In general, with regard to computer crime, Criminalization should be specific, and the law must meet the requirements of clarity and adequacy. Concerning procedural powers, investigative measures must be prescribed by law and pursue a legitimate aim without affecting privacy rights. There must be also a guarantee against abuse, and these procedural powers should be limited to safeguards during the collection of electronic evidence. Regarding human rights, privacy rights, and due process rights the cybercrime legislation incorporates provisions that present a potential threat to the right to privacy and principles of procedural justice. The right to privacy is guaranteed under Article 26 of the Ethiopian Constitution and international treaties such as Art 17 of the International Covenant on Civil and Political Rights to which Ethiopia is a state party. So, there is an incompatibility between the Computer Crime Law of 958/2016 and the constitution, the international Covenant on Civil and Political Rights to which Ethiopia is

[68] *BC. Art 23.*

[69] *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.*

[70] *Cited at note 20*

[71] *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.*

[72] *https://youtu.be/pepOapF_0ds?t=2734, ጠ/ሚኒስትር ዐቢይ አህመድ ከሠ/ተምቤት አባላት ለቀረቡላቸው …… June 14, 2022 | ዓባይ ቲቪ ዜና*

[73] *UDHR. Article 19. and ICCPR . Article 19.*

[74] *. BC. Art (14-15) and ECC. Art (29-38)*

[75] *BC. Art 15*

a state party. Proclamation No.958/2016 should be harmonized with the FDRE Constitution, international covenants on civil and Political Rights, and other regional covenants like the Budapest Convention.