Implications of the Ethiopian Computer Crime Proclamation on the Enjoyment of Human Rights

Shishay Abraha Mehari
Lecturer, Adigart University School of Law

Received: March 12, 2020 Accepted: April 17, 2020

ABSTRACT: *Ethiopia enacted the Computer Crime Proclamation in 2016, aiming to better prevent, protect against and investigate cybercrimes than what the previously enacted laws did. This Proclamation has had positive and negative implications on the enjoyment of human rights. On one hand, the proclamation protects human rights by punishing perpetrators, and on the other hand, it violates human rights by unduly taking this punishment past the tolerable limit. Although it protects rights to property, security and development by creating awareness about potential offenders and punishing criminals, it has eroded many rights, including the right to privacy, the presumption of innocence, freedom of expression, and access to information. The State's excessive emphasis on development and national and political security resulted in the enactment of laws such as the Computer Crime Proclamation 958/2016, which promotes development and security at the expense of human rights. However, nothing is more precious to human beings than human rights. This paper, hence, recommends revision of the Proclamation so as to sufficiently prevent, control, investigate and prosecute the suspects of computer crimes without infringing the above human rights.*

Key Words: *Cyber Law, Cybercrime, Human Rights, Ethiopia*

1. Introduction

Information technology is among the innovations of this era that changed the world into a small village through technological networking. Nowadays, persons in one corner of the globe can access information released on a computer from anywhere else in the world within microseconds, and communicate with people thousands of kilometers away in that time. They can seek, impart and receive an idea without any need to go to its source and can similarly disseminate their ideas easily and swiftly.[1] Therefore, the internet has become a major vehicle for the enjoyment of the right to information and freedom of expression, thereby narrowing the knowledge gap between the developed and underdeveloped world.[2] This is, *inter alia,* the trophy of the era of information brought to humankind in this generation.

Despite the above-mentioned benefits, the information system, best typified by the internet,[3] is susceptible to security threats that can eventually impede the development and security of a State and endanger human rights, such as right to privacy, unless appropriate protection and security measures are taken.[4] Numerous cyber-crimes are committed everyday all over the world, to which Ethiopia is not an exception.[5] The Government, as a duty bearer to control threats to the security of the people, is obliged to identify and

[1] All Answers ltd, *The Internet Has Virtually Reduced the World to a Global Village*(Lawteacher.net, April 2018) <https://www.lawteacher.net/free-law-essays/commercial-law/the-internet-has-virtually-reduced-the-world-to-a-global-village-commercial-law-essay.php?vref=1>. Accessed 23 April 2020.

[2] Australian Human Rights Commission 'Human Rights in Cyberspace'(2013) at 3 <www.humanrights.gov.au>. Accessed on December 1, 2019.

[3] Internet is a global network of interconnected computers, enabling users to share information along multiple channels. See Abebe Regassa, *Introduction to Computer and Internet: Teaching Material for Law Students*, (Sponsored by the Justice and Legal System Research Institute, 2009).

[4] See preambles of the Computer Crime Proclamation, Proclamation No. 958/2016, *Neg. Gaz*, Year 22, No. 83, Protection of Telecommunications and Electric Power Networks Proclamation, Proclamation No, 464/2005, *Neg. Gaz*., Year 11, No. 54, and the Telecom Fraud Offence Proclamation, Proclamation No. 761/2012, *Neg. Gaz*, Year 18 No. 61.

[5] Halefom Hailu, 'The State of Cybercrime Governance in Ethiopia' (2015) at 6 <www.globalnet.org> . Accessed on November 5, 2019.

control cyber-crimes through its legislative, executive and judiciary arms.[6] To this end, the Ethiopian government has enacted several laws and organized institutions of implementation.[7]

A closer look at Ethiopian cyber law in general and the recent Computer Crime Proclamation (or the "Proclamation") in particular, however, shows that some constitutionally-guaranteed human rights are overlooked in the enactment and implementation of these laws. Cyber security laws, just like any other domestic laws, must be designed and implemented in a way that is consistent with international human rights laws, many of which are binding on the Ethiopian state.[8] And, under international law, a state cannot invoke its domestic laws, including its constitution, for its failure to perform a treaty.[9] The Ethiopian House of Federation, a political body, may therefore declare laws that infringe human rights void, since it is required to interpret the constitutional provisions regarding human rights in a manner conforming to international instruments adopted by Ethiopia.[10] Moreover, restrictions on the enjoyment of human rights provided under the Constitution should not be used as an opportunity to claw-back the entirety of the right through subsequent ordinary legislations. Such limitation clauses should not be used as a means to do away with its treaty obligations by giving primacy to domestic laws.[11]

This article starts with what the cyber law system in Ethiopia looks like. It then examines what a limitation to human rights[12] means, how it should be interpreted, and how it interacts with cyber law enforcement. I argue that computer crimes can be controlled without trespassing the bounds of the limitations and derogations of human rights recognized by the Ethiopian constitution and international human rights instruments to which Ethiopia is a party. The main emphasis of this article is to examine the positive and negative implications of the 2016 Computer Crime Proclamation on the enjoyment of human rights. Lastly, this article provides concluding remarks and recommendations for further refinement of the law in a way that conforms to human rights standards.

---

[6] Anja Kovacs and Dixie Hawtin, 'Cyber Security, Cyber Surveillance, and Online Human Rights', at 2 <https://www.gp-digital.org/publication/second-pub/pub/>.S Accessed on April 23, 2020.

[7] Telecom Fraud Offence Protection Proclamation No. 761/2012 and the Computer Crime C are some of the laws, while Public Prosecutor, Police and the Information Network Security Agency are some of the institutions established specifically to prevent and control cybercrimes.

[8] Constitution of the Federal Democratic Republic of Ethiopia proclamation (hereinafter the FDRE Constitution), Proclamation no 1/1995, *Neg. Gaz*., Year 1 No 1, art. 13(2), Consolidation of the House of the Federation and Definition of its Powers and Responsibilities Proclamation No. 251/200 I, *Neg. Gaz.*, Year 7 Year No 41, art.7(2) and Minutes of the Ethiopian Constitutional Assembly, Volume 2, p 68 (Tikimt 30-Hidar 7 1987 EC). Ethiopia has ratified International Covenant on Civil and Political Rights (hereinafter ICCPR) on 11 June 1993, CEDAW on10 September 1981, Convention on the Rights of Children (CRC) on 14 May 199; for more information see United Nations Treaty Collections at:http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&lang=en. Accessed on 23 April, 2020.

[9] Vienna Convention on the Law of Treaties (adopted on 23 May 1969 entered into force on 27 January 1980), art. 27(2). Ethiopia has signed this treaty on 30 April 1970. See https://en.m.wikipedia.org/wiki/List-of-parties-to-the-Vienna-Convention-on-the-Law-of-Treaties. Accessed on April 23, 2020.

[10] The FDRE Constitution (n 8) arts. 13(2), 62(1), 83 and 84(2). For detail information, see Yonatan Tesfaye, 'Whose Power is it anyway: The Courts and Constitutional Interpretation in Ethiopia (2008) Journal of Ethiopian Law, Vol. 22, No. 1, at pp. 128-144.

[11] Abdi Jibril Ali, 'Derogation from Constitutional Rights and its Implication under the African Charter on Human and Peoples' Rights' *(*2013) Law, Democracy & Development, Vol. 17, at 91.

[12] Albeit some human rights are absolute, most of them are subject to limitations. This article is examining how limitations should be inserted in the enjoyment of human rights. Examining limitation to human rights helps to safeguard the right from undue restriction. For instance, the limitations provided to restrict the right to information should not be capable of jeopardizing the essence of the right. Limitations should be necessary, strictly interpreted, and should be compatible with the objectives of the right. Examining limitation to human rights helps to safeguard the right from undue restriction. See UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28, September 1984, E/CN.4/1985/4, part I, A.

2. Recognition of Cyber Law in Ethiopia

Cyber law is an area of law that governs activities connected with computer and internet use.[13] It is a recent area of law that has emerged with the expansive use of digital devices to govern, prevent, and resolve disputes arising from the use of computers and the internet.[14]

Ethiopia, though a country with low internet penetration[15], started enacting cyber-related laws from 2004 onwards, the first being the Criminal Code of the Federal Democratic Republic of Ethiopia 2004, arts. 706 to 711 of which governed computer crimes.[16] This law, however, was limited to governing substantive matters and included only few acts as criminal acts. It criminalized unauthorized access, use and taking of computer services (hacking) under art. 706, causing damage to data (dissemination of malware) under art. 707 and disruption of computer use by authorized users (denial of service attacks) under art. 708, only.[17] A case related with causing damage to data was instituted in Federal First Instance Court in 2014. The Public Prosecutor charged Mr. Yonas Kasahun with contravening art. 707(2) of the FDRE Criminal Code. The latter was accused of intentionally causing damage to a computer system to defraud, deceive or obtain money, property, computer services or any data. He had accessed an e-mail of the victim by using her password without authorization and copied contractual relations she had made with many international organizations and deleted it from the victim's e-mail. Then, he intimidated her saying that he has deleted her e-mail contacts and will only return it if she offer him 50,000,000 Ethiopian Birr. The court has punished Mr. Yonas with 2 years rigorous imprisonment and 5,000 Birr fine after examining evidences of both parties.[18]

The evidence and procedure part that govern cybercrimes together with other crimes was provided under the Criminal Procedure Code of Ethiopia Proclamation No. 185 of 1961[19]. Subsequent laws, especially related to telecommunications, include Protection of Telecommunications and Electric Power Networks Proclamation No. 464/2005, which penalizes theft or intentional destruction or obstruction of telecommunications or electric power networks under its art. 4, and the Telecom Fraud Offence Proclamation No. 761/2012, which criminalizes, *inter alia*, unauthorized service provision, telecom use for illegal purpose, interception and illegal access to telecom system, call-back service, and manipulation or duplication of SIM and credit cards.[20] The latter law provides for the establishment of a special task force to prevent, investigate and control telecom fraud offences, including through covert searches warranted by the court.[21] Electronic evidence and evidence gathered through interception or surveillance are also made

[13] Bryan A. Garner, *Black's Law Dictionary*, (7th edn. West Group, ST. PAUL, MINN., 1999) at 410.

[14] Cyber Law, https://definitions.uslegal.com. Accessed on Nov. 27, 2019.

[15] See Mesenbet A. Tadeg, 'Freedom of Expression and the Media Landscape in Ethiopia: Contemporary Challenges', at 18. <http://ssrn.com/abstract=2763600>. Accessed on November 20, 2019. In 2017, internet penetration is 1.5, which is very low compared to international standards. It has been 1.1 in 2012. See also Kinfe Micheal Yilma, 'Developments in Cybercrime Law and Practice in Ethiopia' (2014) Computer Law and Security Review, at 720.

[16] Kinfe Michael (n 15) at 721. The Telecommunication Proclamation, proclamation No. 49/1996, *Neg. Gaz.*, Year 3, No. 5, which prohibited persons other than employees to connect or disconnect telecommunication lines and the use of call-back service under its art.24 was, however, enacted before the Criminal Code. For definition of "Call-back service", see the definitional part of the Telecom Fraud Offence Proclamation (n 4).

[17] Kinfe Michael Yilma, 'Some Remarks on Ethiopia's New Cybercrime Legislation' (*2016) Mizan Law Review*, *Vol. 10*, *No. 2*, at 448.

[18] Public Prosecutor Vs. Yonas Kasahun Girma, federal first instance court, *file no. 108335*, October 23, 2015. For detail, see Wonber, Alemayehu Haile Memorial Foundation's bulletin, 16th half year, 2015, at pp.52-86.

[19] Halefom (n 5) at 14. The 1961 Criminal Procedure Code which was enacted to enforce the 1957 Penal Code is not amended even after the FDRE Criminal Code 2004 is enacted. Since the notion of cyber law and computer system was not known in Ethiopia during the 1960s, the investigation and prosecution of cybercrimes using the 1961 Criminal Procedure Code was ineffective.

[20] The Telecom Fraud Offence Proclamation (n 4) arts. 3-10. Article 5 of the Telecom Fraud Offence Proclamation No. 761/2012 which deals with offences related to illegal interception in and access of telecom system is repealed by the Computer Crime Proclamation. See Computer Crime Proclamation (n 4), art.43(1).

[21] Id, arts.13 and 14.

admissible under this law.[22] Since the above-stated laws were not adequate to govern the technological changes and sufficiently prevent, control, and investigate cybercrimes and prosecute suspects, a recent Computer Crime Proclamation, which is the principal target of this article, was enacted in 2016.

3. What is Criminalized under the Computer Crime Proclamation?

The new Computer Crime Proclamation has come up with comprehensive provisions broadening the scope of cybercrime in terms of guarantying rights. To list some, it has criminalized illegal access, interception or interference with computer data, system or network, and causing damage to computer data.[23] It further criminalizes computer-related forgery, fraud and identity theft under Arts. 9, 10 and 11, and child pornography, acts against the liberty and reputation of others, and acts against public security under arts. 12, 13 and 14, respectively. It has gone further to criminalize service providers for their participation in and failure to cooperate in the investigation of computer crimes or hindrance of the same. This Proclamation has specifically provided the amount or extent of penalty for each crime. Crimes committed against natural persons are subject to lower punishments than those committed against legal persons.[24] Though the Proclamation is deep in criminalizing several acts, it still needs to criminalize other acts, like disseminating 'racist and xenophobic content, intellectual property related crimes, revenge, pornography and large-scale cyber-attacks through botnets'.[25]

Unlike the Criminal Code of 2004, the Computer Crime Proclamation criminalizes, almost, intentional acts only.[26] Due to the fact that most Ethiopians do not have sufficient knowledge of computer systems,[27] many illicit acts may be committed by negligence or lack of awareness, and punishing everyone who negligently commits computer crimes would be senseless and uneconomic. This is one of the positive provisions introduced by the Proclamation. Negligence is not punishable, except the negligent disclosure or transfer of any computer program, secret code, key, password or any other similar data for gaining access to a computer system, computer data or network specifically stated under art. 7(5) of the Proclamation, though it is hard to distinguish between intentional and non-intentional computer crimes. The punishment of a fine

[22] Id, art. 15. This proclamation was against the right to privacy stipulated under art. 26(2) of the FDRE Constitution, which reads; "Everyone has the right to the inviolability of his notes and correspondence including postal letters, and communications made by means of telephone, telecommunications and electronic devices". It opens the opportunity for the government to easily punish its political dissenters.

[23] See 'Nation Finalizing first-ever Computer Crime Proclamation, *(Ethiopian News Agency, Addis Ababa 13 April 2016.*http://www.ena.gov.et/en/index.php/social/item/1161-nation-finalizing-first-ever-computer-crime proclamation, Tinishu Solomon, 'New Ethiopian Law Targets Online Crime', *(The Africa Report, 09 June 2016)http://www.theafricareport.com/East-Horn-Africa/new-ethiopian-law-targets-online-crime.html*. See also arts. 3, 4, 5 and 6 of the Computer Crime Proclamation.

[24] See Computer Crime Proclamation (n 4) arts. 3 to 6. For example, under art. 4, an illegal interception to computer data owned by natural person is punishable with rigorous imprisonment not exceeding five years, fine from Birr 10,000 to 50,000, but it is punishable with rigorous imprisonment from five years to ten years, and fine from Birr 50,000 to 100,000 if the computer data is destined the use of a legal person.

[25] Kinfe Micheal Yilma (n 17) at 455. However, such acts and acts committed against financial institutions may be included in the proclamation through interpretation. Dissemination of computer system with racist, xenophobic and revenge content, for instance, may fall within crimes against public security, while crimes against intellectual property and financial institutions fall under Section two of the proclamation.

[26] Halefom (n 5)19. See Computer Crime Proclamation(n 4), arts. 3(1), 4(1), 5(1), 6(1), 7(1), 10(2), etc… The only crime by negligence is provided under art. 7(5) of the proclamation, i.e., negligent disclosure or transfer of any computer program, secret code, key, password or any other similar data for gaining access to a computer system, computer data or network.

[27] Only 4.2 % of Ethiopians use computer systems, i.e., 4,288,023 peoples use computer out of the 101,853,268 total demographic size. Ethiopian computer use has only 0.1 world share. See www.inteenetlivestats.com. Accessed on April 29, 2020.

provided in the Proclamation instead of imprisonment is also higher than stated in the Criminal Code of 2004.[28]

4. Limitation On Human Rights and its Justification

The general rule in human rights law is that fundamental rights and freedoms should be protected by the state,[29] while limitations or restrictions are exception to the general rule.[30] However, this does not mean that human rights are absolute. They can be limited and even derogated from in states of emergency, save some non-derogable rights.[31] International instruments and domestic constitutions list rights which are non-derogable, while they provide limitations generally applicable to all rights or specifically in the articles that guarantee those rights.[32] Some rights may be limited for the sake of public order, public health, public morals, national security, public safety, rights and freedoms of others, etc.,[33] save some rights like, freedom from slavery or servitude, freedom from torture and inhuman treatment.[34] Such rights are non-derogable and not subject to limitation. However, for a limitation or restriction to be justified, it needs to be based on certain generally accepted principles. It should be strictly interpreted not to swallow the concerned right, and it must be legal, proportionate, necessary and legitimate.[35] The limitations that are provided as an exception to the enjoyment of the right should not reappear as a principle through subsequently enacted laws so as to detract from the essence of the right intact.

Ethiopia has incorporated human rights under Chapter Three of the Federal Democratic Republic of Ethiopia (herein after FDRE Constitution), providing specific limitations for the rights enshrined therein.[36] All the rights under that Chapter are required to be interpreted in a manner that conforms with the

[28] Illegal access to computer data, for instance, is punishable with fine from Birr 30,000 to 50, 000 under the Computer Crime Proclamation, while it punishable with fine not exceeding twenty thousand Birr under the FDRE Criminal Code. See art. 3(1) of the Computer Crime Proclamation and art. 706(2) of the Criminal Code respectively.

[29] It can also be argued that, in addition to the state, all citizens, political organizations, other associations are duty bound to protect human rights. The FDRE Constitution obliges them to ensure the observance of the constitutional provisions, two-third of which deals with human rights. See art. 9(2) of the FDRE Constitution.

[30] Nihal Jayawickrama (2002), cited in Abdi Jibril Ali, 'Distinguishing Limitation on Constitutional Rights from their Suspension: A Comment on the CUD Case (2012), Haramaya Law Review, Vol. 1:2, at 5.

[31] The ICCPR prohibits derogation from its art 6 (right to life), Art 7 (prohibition of torture), art 8 (prohibition of slavery and servitude), art 11 (prohibition of imprisonment for inability to fulfill contractual obligation), art 15 (prohibition of retrospective criminal law), art 16 (right to be recognized as a person), and art 18 (freedom of thought, conscience and religion). See also arts. 93(4 (C)) and 13(2) of the FDRE Constitution cumulatively. Art. 93(4(c)) of the FDRE Constitution has listed only four rights as non-derogable. Right to life, freedom of thought, conscience and religion, and prohibition of non-retroactivity of criminal law are not included in the list of non-derogable rights. However, since art. 13(2) of the Constitution urges the interpretation of human rights provisions in a manner that conforms international human rights treaties to which Ethiopia is a party, it is sound to argue that such rights are non-derogable through interpretation.

[32]Abdi Jibril Ali (n 29) at 5.

[33] The Siracusa Principles (n 12) part I, B.

[34] Convention Against Torture And Other Cruel, Inhuman Or Degrading Treatment Or Punishment, adopted by the UN General Assembly in resolution 39/46 of 10 December 1984 at New York , art. 2(2). It reads "No exceptional circumstances whatsoever, whether a state of war or a threat of war, internal political instability or any other public emergency, may be invoked as a justification of torture.' *See* also ICCPR art. 7 and the ACHPR, art. 5. The FDRE Constitution art.18 also does not provided limitation on such rights.

[35] Siracusa Principles (n 12) part I, A. In case of derogation, a situation should be sufficient to declare a state of emergency and the derogation that follows should be 'strictly required by the exigencies of the situation' in its severity, duration, and geographic scope. ICCPR General Comment No. 29: article 4: Derogations during a State of Emergency, Adopted at the Seventy-second Session of the Human Rights Committee, on 31 August 2001 ICCPR/C/21/Rev.1/Add.11, General Comment No. 29. (General Comments), and the Siracusa principles, part II.

[36] See the FDRE Constitution (n 8) arts. 15, 17(1), 19(6), 26(3), 27(5), 29(6), etc…

international human rights conventions to which Ethiopia is a party.[37] Hence, the validity and legitimacy of laws that limit the enjoyment of human rights are to be examined with reference to the FDRE Constitution and the international human rights conventions ratified by Ethiopia.

The Computer Crime Proclamation is one of the laws that limit the enjoyment of human rights for reasons of development of the State and protection of individual rights. The question is whether it is reasonable, under human rights standards, to completely erode rights to protect some individual and state interests. Protection of some individual rights and state interest should not be at the expense of other rights. A certain law may protect some individual rights by suspending other rights. For instance, right to security may be protected by limiting the right to privacy. However, laws should be enacted to balance several rights as far as possible and limitations should be proportional only to the extent necessary to protect other rights. If a certain right can be protected without the need to limit other rights, no limitation should be placed on the enjoyment of such other rights.[38]

5. Positive Implications of the Computer Crime Proclamation on Human Rights

The Computer Crime Proclamation came into effect to protect numerous interests by limiting individual rights. Limitation of one's rights could be justified in some cases where it advances the protection of others' rights,[39] and if the legal and institutional arrangement to enforce the Proclamation is capable of striking a balance between the limitation of some rights and the objective of such limitation. In safeguarding some rights and interests, the limitation on other rights should be to the extent necessary to do so. The Proclamation seeks to safeguard the following interests.

5.1 National security

Though the State as an entity is not a human rights holder,[40] violations against the State have the potential to threaten the enjoyment of human rights by individual or group of persons in that state. Acts against the state's economy and security devalues human rights directly or indirectly. For instance, though terrorism is targeted on the state, it has a direct impact on the enjoyment of a number of human rights, in particular, the rights to life, liberty and physical integrity.[41]

Unless the cyber security is well protected, it has the potential to bring chaos and disorder that wears away human rights enjoyment. Individuals and groups may disseminate computer data that incite violence and public unrest. This is criminalized with rigorous imprisonment not exceeding three years under the Proclamation.[42] Freedom of expression is not an absolute right. It is subject to limitation; to protect the rights or reputations of others, to protect national security, public order, public health, morals, etc.[43] The

[37] The FDRE Constitution (n 8), art 13(2).

[38] Julie Debeljak, 'Balancing Rights in a Democracy: The Problems with Limitations and Overrides of Rights under the Victorian Charter of Human Rights and Responsibilities Act 2006' (2008) Melbourne University Law Review, Vol. 32, at 426. The balance of a certain limitation can be assessed based on the nature of the right; the importance of the purpose of the limitation; the nature and extent of the limitation; the relationship between the limitation and its purpose; and any less restrictive means reasonably available to achieve the purpose that the limitation seeks to achieve — a minimum impairment test.

[39] Universal Declaration of Human Rights, adopted and proclaimed by the UN General Assembly in resolution 217 A (III) of 10 December 1948 at Paris, art. 29(2). It reads "…In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society".

[40] From the human rights perspective, only human beings are rights-holders, while the state is a duty bearer for the enjoyment of such rights by human beings. See Rights Holders, <socialprotection-humanrights.org.>. Accessed on April 29, 2020.

[41] Office of the United Nations High Commissioner for Human Rights, Peace and Security Section of the Department of Public Information, 'Fact Sheet No. 32: Human Rights, Terrorism and Counter-terrorism' (July 2008) United Nations, Geneva, 7.

[42] The Computer Crime Proclamation (n 4), art. 14.

[43] See ICCPR (n 8) art. 19 (3), and the FDRE Constitution (n 8), art. 29(6).

Computer Crime Proclamation also safeguards security by penalizing illegal use of computer systems for the purpose of instigating war, terror and hostility among the people. It reads:

> *… [w]hosoever intentionally disseminates through a computer system any written, video, audio or any other picture that incites violence, chaos or conflict among people shall be punishable with rigorous imprisonment not exceeding three years.*[44]

However, there is a risk that this limitation may be used for political gain by certain parties, due to the subjective nature of the concept of public security. Since the type of expressions that incite chaos and disorder depend upon the political climate, expressions which are unfriendly to the Government but with no propensity to endanger public security has the potential to be twisted and characterized as incendiary.[45]

5.2 Development

It is evident that information and communication play a pivotal role for the economic, social and political development of a State (since the development of the state is the cumulative effect of the development of the people).[46] At the same time, it is vulnerable to crimes and security threats that require prevention and control.[47] Offenders intercept and damage computer systems that are designed to foster the development of individuals, and take advantage of others through computer forgery and fraud. Such acts are criminalized under arts. 9 to 11 of the Proclamation to protect the right to development of individuals in particular and of the state in general. A computer damage (altering, deleting, suppressing a computer data, rendering it meaningless, useless or inaccessible to authorized users) on individual's developmental activities without authorization or in excess of authorization is also punishable.[48] By penalizing such acts, the Proclamation has tried to safeguard the right to development of individuals and the interest of the state.

5.3 The right to liberty and reputation

Liberty and reputation are the other human rights that get protection under the Proclamation.[49] Such rights are protected through preventing violation of the right, giving prior notice of what acts are punishable, and punishing transgressors. Art. 13 of the Proclamation penalizes one who intimidates or threatens another through computer systems. Disseminating any writing, video, audio or any other image through a computer system that intimidates or threatens another person or his families with serious danger or injury is punishable with rigorous imprisonment up to five years.[50] Any writing, video, audio or any other image through a computer system that is defamatory to the honor or reputation of any person is also punishable with simple imprisonment up to three years or fine up to Birr 30,000 or both.[51] In addition to the criminal penalty, the state has an international obligation to ensure that anyone whose rights are violated gets an effective remedy.[52] The defendant compensates the victim with civil damages equal to the damage the latter has sustained.[53] By doing so, the law safeguards liberty and reputation of persons.

6. Negative Implications of the Proclamation on the Enjoyment of Human Rights

This is an attempt to amplify the negative impact of the Proclamation on certain human rights. The Proclamation has drawbacks, especially in its evidentiary and procedural part, which provides a benchmark

[44] The Computer Crime Proclamation (n 4), art.14.

[45] There are pending cases in the Federal Attorney General Lideta Branch (Addis Ababa, Ethiopia) related to this issue. I could not use them in this paper for the sake of the proper function of the justice system, since the case is not decided.

[46] See preamble of the Computer Crime Proclamation (n 4).

[47] Computer Crime Proclamation (n 4), preamble. A certain case related with interception in bank account, by a student of a certain Ethiopian University, is pending during the time this paper is written.

[48] The Computer Crime Proclamation (n 4), art. 6(1).

[49] The Computer Crime Proclamation (n 4), art. 13. Everyone has the right to respect for his reputation. See art. 24(1) of the FDRE Constitution, UDHR, art. 12, ICCPR, art. 17. The right to liberty is also recognized under art. 17 of the FDRE Constitution, art. 3 of the UDHR, and art. 9 of the ICCPR.

[50] The Computer Crime Proclamation (n 4), art. 13(1).

[51] Id, art. 13(3). A certain case that is related with disseminating video on Facebook that shows a naked woman is pending in Lideta Federal High Court, Ethiopia.

[52] See art. 2(3) of the ICCPR and art. 8 of the UDHR. See also the Criminal Code of the Federal Democratic Republic of Ethiopia, 2004, art. 101, Civil Code of the Empire of Ethiopia Proclamation No. 165 of 1960, art. 2035.

[53] Civil Code of the Empire of Ethiopia, art. 2091.

principle of how computer crime prevention, investigation and evidence procedures shall be implemented, stating that;

> *[T]he prevention, investigation and evidence procedures provided in this Part and Part Four of this Proclamation shall be implemented and applied in a manner that ensures protection for human and democratic rights guaranteed under the Constitution of the Federal Democratic Republic of Ethiopia and all international agreements ratified by the country.*[54]

Despite this statement, the provisions that follow are not inserted in a way that conforms to the referenced principle. The statement, therefore, seems like a 'sham clause'.

Laws are enacted by the Ethiopian government to restrain the enjoyment of human rights for a number of reasons. First, the state policy which gives priority to development, having 'economic growth first'[55] as a motto, emphasizes economic development even at the expense of human rights. This is something Ethiopia has copied from the East-Asian countries as a model for economic policy.[56] However, this policy is irreconcilable in a State that devotes one-third of its constitution to human rights protection, stating that those rights are inviolable and inalienable; it is therefore incompatible to prioritize economic growth over human rights.[57] Otherwise, there should be legal and institutional apparatus that balance such rival concepts.[58] Second, the Ethiopian government retains its right to suppress political protest.[59] It has enacted several human-rights-unfriendly laws to decimate political dissent.[60] The Vagrancy Control Proclamation, the Freedom of the Mass Media and Access to Information Proclamation, the Proclamation to Provide for the Registration and Regulation of Charities and Societies, and the Anti-Terrorism Proclamation are among the draconian laws which have excessively limited the enjoyment of human rights and political horizon.[61] The computer crime law is an extension of this anti-human rights process. Some of the rights infringed in the Proclamation are discussed below.

6.1 The right to privacy

The right to privacy is incorporated under several human rights instruments,[62] as it is central to human dignity and reinforces the enjoyment of other rights, such as freedom of expression and information.[63] This celebrated right is endangered by the Computer Crime Proclamation through;

6.1.1 Cyber surveillance

In a State where demonstration and petition, let alone dissenting political views, are labeled as acts of terrorism, people tend to use other ways to convey their views incognito. However, there is a fear of surveillance and electronic filtration that the Government conducts clandestinely.[64] Ethiopia, despite its

---

[54] The Computer Crime Proclamation (n 4), art. 21.

[55] Amartya Sen (1999); cited in Assefa Fiseha Yeibyio, Ethiopia Development with or without Freedom?, in *Human Rights and Development Legal Perspectives from and for Ethiopia*, International Studies in Human Rights (2015), Vol. 111, at pp. 101-138.

[56] Ethiopia's Search for Alternative Exemplars of Development, www.open.ac.uk. Accessed on April 12, 2020.

[57] World Bank, Human Rights and Economics: Tensions and Positive Relationships, at 11. Available on http://siteresources.worldbank.org/PROJECTS/Resources/40940133106826855 8/Report Development Fragility human Rights.pdf. Accessed on May 4, 2020.

[58] Assefa Fiseha Yeibyio, 'Ethiopia Development with or without Freedom? In: *Human Rights and Development Legal Perspectives from and for Ethiopia*, (International Studies in Human Rights 2015, Vol. 111), at 130.

[59] Human Rights Situation in Ethiopia, Unrepresented Nations and Peoples Organization, unpo.org. Accessed on 23 April, 2020.

[60] Mesenbet (n 15) at 18.

[61] Vagrancy Control Proclamation No. 384/2004, *Neg. Gaz.*, 10th Year No. 19, Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, *Neg. Gaz.*, 14th Year No. 64, Charities and Societies Proclamation No. 621/2009, *Neg. Gaz.*, 15th Year No. 25, and Anti-Terrorism Proclamation No. 652/2009, *Neg. Gaz.*, 15th Year No. 57, respectively. For detail information, see Mesenbet (n 15).

[62] See art. 12 of the UDHR, art. 17 of the ICCPR, art. 10 of the ACHPR, and art. 26 of the FDRE Constitution.

[63] Stakeholder Report Universal Periodic 27th Session, *The Right to Privacy in India*, (2016) at 2.

[64] The Ethiopian government uses internet filtration through the government monopolized ethio-telecom. Moreover, it undertakes extensive surveillance on political dissidents and journalists. See Mesenbet (n 15) at 21. Though interception and access in computer systems without authorization is illegal, it is 'legalized' when the

very limited telecoms infrastructure, has introduced advanced 'surveillance technologies including the FinFisher malware from the Italian based IT company Hacking Team to track political dissidents and journalists both inside and outside the country'.[65] The Proclamation allows investigatory organs to intercept or conduct surveillance of the computer systems of suspects, even without court warrant, upon permission by the Attorney General, when it is reasonable that a computer crime that damages 'critical infrastructure' is or is to be committed.[66] Both 'critical infrastructure' and 'reasonable' are vague and can be misused, since it is the Attorney General, a government official, that grants and rejects requests for interception or surveillance.

6.1.2 Sudden search and digital forensic investigation

The Proclamation provides that sudden searches or digital forensic investigations may be conducted on computer systems or data when there is a reasonable suspicion that a computer crime is to be committed.[67] This may have the positive implication in providing early warning to citizens as stated in the law, but since it is to be conducted without the knowledge of the targeted person, it is far from complying with the limitation clause under art. 26 of the FDRE Constitution, which should be strictly interpreted.[68]

What is worse is that, under art. 32 of the Proclamation, the law allows investigations to be conducted through physical as well as virtual access or searches on any computer system. Such virtual digital investigation poses a danger to privacy rights, since the court does not have oversight mechanisms.[69] The Information Network Security Agency (INSA) Reestablishment Proclamation No. 808/2013 had granted power to the INSA to conduct "digital forensic investigation *without physical presence*"[70]. (Emphasis added) The other problem here is that the Proclamation allows 'general search warrant'.[71] The investigation may extend to other computer systems without requesting separate search warrants, where there is a belief that the computer data is stored in another computer system.[72] This provision circumvents the other provisions requiring search warrants, and so arbitrarily restricts the inviolable right to notes and communications by means of electronic devices.[73]

6.2 The right to expression and access to information

Freedom of expression and access to information is among the central civil and political rights.[74] It is central as it is a prerequisite for the search of truth, self-governance and personal development more than other rights can do.[75] Creating an open environment for public discussion helps to reach a rational decision

government intercepts in a computer data of a suspect without the authorization of the latter. See art. 3 and 4 , 13(2) cumulatively with art. 25 of the Computer Crime Proclamation.

[65] Mesenbet (n 15) at 21. A certain political dissident, Mr. Kidane, a US resident, had lodged a complaint to the state of Colombia against the Ethiopian government for violation of his privacy committed through surveillance by the latter. See Kidane v. Fed. Democratic Republic of Eth., No. 14-cv-372 (D.D.C. 2015), available at https://www.eff.org/cases/kidane-v-ethiopia.

[66] The Computer Crime Proclamation (n 4) art. 25(3).

[67] Id, art. 26(1). Digital forensics is the process of uncovering and interpreting electronic data by collecting, identifying and validating the digital information for the purpose of reconstructing past events. See Data Forensics, https://www.techopedia.com/definition/27805/digital-forensics. Accessed on May 4, 2020.

[68] It is rule under human rights law to interpret limitations of human rights strictly and the sudden search and investigation should be conducted in a way that does not infringe rights to privacy, honor and reputation of the targeted person. See Siracusa Principles (n 12) part I(A(3)).

[69] Knife Micheal (n 10) at 453.

[70] The Information Network Security Agency (INSA) Reestablishment Proclamation No. 808/2013, *Neg. Gaz*., Year 20, No. 6, art. 6(8). The suspect does not have knowhow as to what is undertaken on his corresponding.

[71] The Computer Crime Proclamation (n 4), art. 32(2).

[72] Ibid.

[73] *See* the FDRE Constitution (n 8), art. 26(2).

[74] Freedom of expression and access to information is recognized under art. 19(2) of the ICCPR, 13(1) of the CRC, 13(2) of International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, art. 7 of the ACHPR and art. 29 of the FDRE Constitution.

[75] Gedion Timothewos, 'Freedom of Expression in Ethiopia: The Jurisprudential Dearth' (2010) Mizan Law Review, Vol. 4 No. 2, at pp. 202-204.

thereby fostering democracy and transparency.[76] Ronald Coase has stated that 'similar to the market place for goods where competition between different business entities enhances pricing and helps in the growth of national economies, freedom of expression also affords individuals the opportunity to contribute different ideas in the economic, social and political life of a community'.[77] It also plays an important role in fostering government accountability by serving as a check on abuse of authority.[78] The exercise of such a right is advanced by the internet system.[79] Therefore, the right to freedom of expression and access to information that people have offline must also be protected online also.[80]

The political reality in Ethiopia reveals that the rights to demonstration, assembly and petition are less tolerated by the government.[81] As such, computer systems constitute perhaps the best mechanism to exercise such rights under the circumstance. The FDRE Constitution has provided that limitation on freedom of expression and access to information should be "guided by the principle that freedom of expression and information cannot be limited on account of the content or effect of the point of view expressed".[82] However, the government seems to put a blanket denial on the enjoyment of these rights in this way. The Computer Crime Proclamation warns individuals not to express their socio-political views, by providing magnetic words, such as, chaos, violence and conflict, which trap acts under crimes against public security.[83] The subjectivity of the words, therefore, creates an opportunity for the government to twist activities the way it likes through broad or strict interpretation of such words.

Therefore, since restricting expression because people have a different style of life or have a different understanding of a certain issue violates autonomy and moral independence of individuals[84], curtails the development of democracy, and search of truth, any limitation on such right has to be considered that it has substantial effects on the enjoyment of other rights also.

6.3 The right to be presumed innocent

This right is among the core principles of human rights that are guaranteed under many human rights laws.[85] Accused persons have the right to be presumed innocent until proven guilty, to remain silent and not to be compelled to testify against themselves.[86] This right does not have exceptions or limitations.[87] Since the accused is presumed innocent, it is the public prosecutor that must prove every element of the crime that the suspect is alleged to have committed, beyond reasonable doubt.[88]

The Proclamation, under art. 37(1), says that the prosecutor has the burden to prove material facts of the case. However, it also states that:

---

[76] Thomas Scanlon, A Theory of Freedom of Expression (1972), Philosophy & Public Affairs, Vol. 204, No. 1, at 216.

[77] Ronald Coase, 'The Market for Goods and the Market for Ideas' (1974), American Economic Review Vol. 64, at 384.

[78] Mesenbet (n 15) at 6.

[79] Navi Pillay, 'Human Rights and the Rule of Law in a Digital Age' (United Nations Human Rights office of the High Commissioner 2013) at 10.

[80] United Nations Human Rights Council 'The Promotion, Protection and Enjoyment of Human Rights on the Internet, Human Rights Council Resolution UN 20/8, Doc A/HRC/RES/20/8' (2012) paragraph 1. <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8>. Accessed on 13 April 2020.

[81] Many demonstrations were disallowed, a recent example being the demonstration called on November 4, 2017 in Mekelle, by Arena Tigray for Democracy and Sovereignty.

[82] The FDRE Constitution (n 8), art. 29(6).

[83] See the Computer Crime Proclamation (n 4), art. 14.

[84] Ronald Dworkin, *A Matter of Principle* (Harvard University Press 1985) at 353.

[85] *See* art. 11(1) of the UDHR, art. 14(2) of the ICCPR, art. 7(1) (b) of the ACHPR, art. 20(3) of the FDRE Constitution.

[86] Ibid.

[87] Ibid. There is no limitation to presumption of innocence under the international human rights instruments and the FDRE Constitution.

[88] Simeneh Kiros, 'The Principle of the Presumption of Innocence and its Challenges in the Ethiopian Criminal Process' (2012) Mizan Law Review, Vol. 6 No. 2, at 16.

> *[N]otwithstanding the provisions of sub-article (1) of this Article, upon proof of basic facts of the case by the public prosecutor if the court believes necessary to shift the burden of proofing to the accused, the court may do so.*[89]

Is it the court that determines who shoulders the burden of proof? The answer is in the negative. The Constitution has already determined it. The constitutional right to presumption of innocence has two aspects; it imposes the burden of proof on the prosecutor and requires the same to prove the guilt of the accused beyond reasonable doubt.[90] The court does not have the power to shift such burden. The Constitution orders courts to presume the innocence of the accused, and not to 'presume guilt'. The court is presuming the guilt of the accused and requiring him/her to disprove it, when it transfers the burden to the latter. Whether 'necessary' or not, the court cannot do so.

Why does the law require transferring the burden of proof to the accused? It may be because the investigation body does not have enough expertise to prove elements of computer crime due to its sophisticated nature. Assume that Mr. X, a layman, is accused of disseminating a hostile video and the burden of proof is shifted to him. How can he prove that it is 'hackers' that disseminated it on his, let us say, Facebook or Twitter account. When the court shifts the burden, it holds him guilty forthwith, since it is hard for a layman disprove his guilty. It is unthinkable for an ordinary citizen to disprove that it is not him/her that disseminated an idea on a computer system, which is too difficult to be proved through the strong task force of the government, i.e., the police, the Information Network Security Agency, public prosecutor and related organs established under the proclamation[91].

Violation of the right to be presumed innocent destroys the right to a fair trial. Due to the indivisible, interdependent and interrelated nature of human rights,[92] the violation of one right, especially the right to be presumed innocent, causes the violation of other several rights, like the right fair trial and right to bail.[93]

The Proclamation states that the court can order *a person* with possession or control of specified computer data to produce it or give access to the investigatory organ.[94] Halefom, looking on the draft Proclamation, has argued that if the phrase *'a person'* in the provision includes the suspect, it is against the constitutional provision which provides freedom against self-incrimination.[95] The provision, especially the Amharic version, states that *'it does not need to call the concerned suspect'* (literal translation mine) departing from the English version which says *"without requiring the appearance of the person"* and connotes that the court orders others only if it does not need the appearance of the suspect. Even if the law is interpreted to allow courts to order a person other than the suspect, such provision produces another risk, i.e. ordering production of evidence in the absence of the concerned person, thus violating their due process and data privacy rights.[96]

7. Conclusion

The Computer Crime Proclamation limits the enjoyment of human rights. Despite it has positive sides for the protection of human rights by creating awareness, deterring perpetrators from further violation of the rights of others and holding them accountable for crimes and trying not to rush to apprehend individuals for negligent acts, it goes beyond the purpose of limitation of human rights.

The Proclamation has several downsides that restrict human rights protection. This article has tried to pinpoint the major problems of the Proclamation from a human rights angle. First, the instrument confers broad powers of surveillance, physical and virtual sudden searches, and digital forensic investigations to the investigatory bodies, which opens the way for the violation of the right to privacy. Second, it is open to

[89] The Computer Crime Proclamation (n 4), art. 37(1).

[90] Wondewossen Demissie, *Ethiopian criminal procedure*, (USAID 2012) at 55.

[91] The Computer Crime Proclamation (n 4), art. 41.

[92] The Vienna Declaration and Programme of Action, adopted by the UN World Conference on Human Rights (157/93), art. 5.

[93] When an accused is presumed guilty, his rights to fair trial and bail as well as the due process of law may fall at stake. For the relation between such rights, see Kelali Kiros, *The Bail Justice in Ethiopia: Challenges of its Administration*(A Thesis Submitted to the School of Law of Addis Ababa University in Partial Fulfillment of the Requirement of Master Degree in Constitutional and Public Law, 2011) at 54.

[94] The Computer Crime Proclamation (n 4), art.31 (2).

[95] Ibid.

[96] Kinfe Micheal (n 17) at 454.

violations of the rights to freedom of expression and access to information. It uses broad terminologies that can be easily abused, especially to punish political dissident. Hence, the Proclamation can be a mechanism to control protests and limit the political rights that are crucial to enhance democratic governance. Third, it inflicts a 'massive blow' on the right to fair trial. It erodes the right to be presumed innocent by granting discretion to the court to shift the burden of proof from the prosecutor to the accused and orders the accused to produce evidence against himself/herself (or requires production of evidence in his/her absence).

Finally, the proclamation leaves some dangerous computer acts, such as the dissemination of racist and xenophobic content, intellectual property related crimes, revenge-pornography and large-scale cyber-attacks through botnets unregulated.[97]

Consequently, the law, as it stands, does not appear to strike a proper balance between its preservation of rights and interests and the broader protection of human rights. In order for this challenge to be addressed, the law should be articulated in a manner that advances human rights protection without bypassing the legitimate human rights limitations. It should be reviewed in a way it advances the protection of human rights, recognized under international and regional human rights instruments as well as the FDRE Constitution (the national grand law), by avoiding its chilling effects on the enjoyment of several human rights.

[97] Id, at 455.