International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicjournal.in
Volume 3; Issue 6; November 2018; Page No. 126-131

Ethiopia computer crime law in light of international human right laws: A critical analysis

Tadesse Woldesenbet Gallo[1], D. Surya Prakasa Rao[2]
[1] Research Scholar in Law, Andhra University, Visakhapatnam, Andhra Pradesh, India
[2] Principal AT Dr. B.R. Ambedkar College of Law, Andhra University, Visakhapatnam, Andhra Pradesh, India

Abstract
Ethiopia computer crime proclamation deals with burning issues, ranging from an illicit access to computer systems to disseminating spam and fighting against child pornography. Further, the proclamation establishes a number of novel criminal activities that are probably to impact on the enjoyment of constitutionally guaranteed rights like right to privacy and freedom of expression. The Internet is fast becoming a way of life for a number of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has facilitated the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind. Internet has entered in all the spheres of human life because the digital world came into existence. The fields like trade, education, corporate sectors, transportation, and communication are highly prejudiced by internet. Internet plays an essential role to make human beings comfortable in their routine life. The computer crime has, of course, become the most occurring instance currently. An internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. It has become a place to do all sort of activities which are prohibited by law. It is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy and corporate espionage, to name a few. There is hardly any human activity that is not touched by the internet. Institutions that follow up cases of computer crime have been vested the power to control nationwide computer crimes. The author of the article suggests that the provisions of the computer law are made so strict that it might impede constitutionally guaranteed human and democratic rights of citizens especially right to privacy and freedom of expression.

Keywords: computer crime, international human rights law, investigation, evidence, jurisdiction, punishment, prosecution, national executive task force

1. Introduction

Background and Objective of the study

Computer crime is a new form of crime in case of Ethiopia. It has been introduced by the Criminal Code of the Federal Democratic Republic of Ethiopia 2004 [1]. It is a description applied to new ways and means of perpetrating peculiar crimes of various kinds, primarily envisaging money laundering, national security threats, illegal interception, electronic identity theft, interference with computer system, causing damage to computer data, child pornography, crime against liberty and reputation of persons and so forth. Many of these crimes are well known, their jurisprudence is well construed and they arise in this context mainly from human greed. Electronic ways of committing them, however, are new and modern crimes against the operation of computer technology itself are as new as the technology. The common feature is the use of information technology in their commission.

However, the methods of prosecution and judicial disposition of cases of computer crimes are basically diverse from those for already established in the FDRE criminal code of 2004 and related laws, novel practical challenges do need to be addressed by public prosecutors and investigatory organs. Conventional legal concepts continue to apply, but always there is need for the creation of specific unimaginable crimes and new procedural rules envisaging evidence law to enable an effective response to new methods of offending by the use of new technology. All that is needed to commence a computer crime are computer and internet systems. The way of committing crime has been exploited by everyone from enthusiastic amateurs to terrorists and with international drug and money traffickers, smugglers and criminal gangs, and some youngsters', antagonist political activists (but not exclusively.) Pursuant to the preamble of the Computer Crime Proclamation No.958/2016 information and communication technology plays pivotal roles in the economic, social and political development of the country [2] and at the same token the preamble gives emphasis on unless appropriate protection and security measures are taken the utilization of ICT is vulnerable to various computer crimes that can hinder the overall development of the country and endanger individual rights [3]. The Concept of paragraph of computer crime

[1] See, the preamble of the FDRE criminal code proclamation no.414/2004 para2 and Articles 706 to 711 which has been repealed by the article 45(1) of computer crime proclamation no.958/2016.

[2] See, Preamble of the FDRE computer crime proclamation no.958/2016 para1.

[3] See Id, preamble, Para2.

proclamation should be construed as human beings are vulnerable so rule of law is required to protect them. Applying this to the computer crime I would argue that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The grounds for the vulnerability of computers might be justified as first the Capacity to store data in comparatively small space. This indicates the computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier. Second justification can be simple to access the problem encountered in guarding a computer system from unauthorized access is that there is plausibility of breach not due to human error but due to the complex technology. By clandestinely implanted logic bomb, key loggers that can steal access codes advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

Another ground would be its complexity meaning the computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is weak and it is hardly plausible that there valor not be a lapse at any stage. The computer perpetrators take advantage of these lacunas and infiltrate into the computer system. Fourthly, negligence is very closely associated with human conduct. It is therefore very probable that whilst protecting the computer system there could be any negligence, which in turn provides a computer perpetrator to gain access and control over the computer system. Last but not lest loss of evidence is a very common and apparent difficulty as all the data are normally destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

The Preamble further elucidates the existing laws are not adequately turned with technology changes and are not sufficient to prevent, control, investigate and prosecute the suspects of computer crimes [4]. Thus this article is devoted to analyze the statutory provisions of the Ethiopia computer crime proclamation of 2016 in light of international human rights laws. The solely feasible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and more making the application of the laws more stringent to check crime. Undeniably the computer crime proclamation is a historical step in the country. Further I argue that there is a need to bring changes in the ICT by amending the first statutory provisions enshrined in FDRE criminal code of 2004.Although those provisions have been the first legal framework to introduce the concept of computer crime in the legal history Ethiopia but I would like to shed on a word of caution for the pro-legislatives that it should be borne in mind that the provisions of the computer crime are not made so stringent that it might retard the right of thought, opinion and expression [5] and the right to privacy [6] enshrined under the FDRE constitution. The principal ground of observing this computer crime proclamation in the perspectives of international instrument is that the right to freedom of expression is protected by a number of international human rights instruments. These comprise in particular article 19 of the Universal Declaration of Human Rights (UDHR) [7] and Article19 of the International Covenant on Civil and Political Rights (ICCPR) i.e. the freedom of opinion and expression [8] as well as at the regional level article 9 of the African charter on Human and peoples' rights (ACHPR) [9]. The ICCPR and ACHPR are binding international treaties ratified by Ethiopi [10] the freedom of expression guarantee in the UDHR is binding on Ethiopia as a rule of customary international law [11] and pursuant to FDRE constitution all international agreements ratified by Ethiopia are an integral part of the law of the land [12]. The same constitution stipulates the fundamental rights and freedoms specified in this Chapter shall be interpreted in a manner conforming to the principles of the Universal Declaration of Human Rights, International Covenants on Human Rights and international instruments adopted by Ethiopia [13]. On other hand, September 2011 report, the Special Reporter elaborated that the scope of legitimate limitations on different types of expression online and identified three different types of expression for the purposes of online regulation:-

1. Expression that constitutes an offence under international law and can be prosecuted criminally.
2. Expression that is not criminally punishable but may justify a restriction and a civil suit; and.
3. Expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others. The Special Reporter elucidated that the solely exceptional types of expression that States are required to proscribe under international law are: (a) child pornography; (b) direct and public incitement to commit genocide; (c) hate speech; and (d) incitement to terrorism [14].

Accordingly, the principal objective of this analysis is to decipher the consistency of statutory provisions of computer crime proclamation in light of international human rights laws.

2. Basic concept of computer crime in Ethiopia

A computer crime is the latest and maybe the most convoluted crisis in Ethiopia. The author of this article hereinafter may use the computer crime interchangeably with cyber crime since the concept of cyber crime is not radically different from the computer crime. Computer crime might be said to be those

[4] Id, preamble, Para3
[5] FDRE constitution (1995),Article 29
[6] Ibid, Article 26

[7] See, UN General Assembly Resolution 217A (III), adopted 10 December 1948.
[8] Adopted by UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976
[9] African charter on Human and peoples' rights adopted 27 June 1981,
[10] Ethiopia acceded to the ICCPR on 11 June 1993 and to the ACHPR on 15 June 1998.
[11] Whereas not a binding document at its adoption, core parts of the UDHR, including the right to freedom of expression, are widely recognized to have acquired the force of customary international law. See e.g. Filarial vs. Pena-Irala, 630 F.2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit)
[12] See, FDRE constitution Article 9(4)
[13] Ibid,FDRE constitution, Article 13(2)
[14] See, Report of the UN Special Reporter on Freedom of Expression (May 2011), Para18.

species, of which, genus is the conventional crime [15], and where either the computer is an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetrating more crimes comes within the ambit of computer crime. A widespread definition of computer crime might be illegal acts wherein the computer is either a tool or target or both. Thus computer crime is use of computers and networks to perform illegal activities such as spreading computer virus, online illegal content data [16], performing unauthorized electronic identity theft [17], illegal computer content data disseminated through a computer, computer system, or computer network [18], illegal access [19], illegal interception [20], interference with Computer System, [21] crimes against liberty and reputation of persons [22] are few mentioned.

Put simply, computer crimes can be perpetrated computer as an instrument and as a target. These could be realized that once a person is the main target of computer crime; the computer can be considered as an instrument rather than the target. These crimes usually envisage less technical expertise as the damage done reflects itself in the real sphere. Human weaknesses are normally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more complicated. These are the offences which have existed for centuries in the offline. Scams, theft, and the likes have existed even prior to the development in high-tech equipment. The same offender has easily been granted an instrument which facilitates his potential pool of fatality and makes him all the harder to trace and apprehend.

On the other hand, computer as a target crime could be perpetrated by a selected group of perpetrators. Unlike offences using the computer as an instrument, these crimes require the technical knowledge of the perpetrators and tactics. These crimes are comparatively new, having been in existence for solely as long as computers have which elucidates how ordinary people and the globe in general are towards fighting against these crimes. There are a number of crimes of this nature perpetrated daily on the internet.

3. Scope and Analysis of computer crime provisions

The computer crime proclamation no.958/2016 of Ethiopia can be classified into six sections. Such as:

A. General Provisions and Definitions

The introductory part begins with article1 which articulates about the nomenclature of the proclamation that is said to be Computer Crime Proclamation No.958/2016. Article 2 deals with the connotations of the words and phrases to be found in the proclamation.I argue that the content of the computer crime proclamation is directly interconnected with human rights law, at least a clause ought to be inserted requiring that the proclamation be interpreted in pursuance to human rights standards, specifically the rights to privacy and freedom of expression. This would also give effect to the African Union Convention on Cyber Security and Personal Data Protection [23] which requires all states Parties to guarantee that measures implemented for the protection of cyber security do not violate human rights laws [24].

B. Computer Crimes

Computer crime has been defined as envisaging any proscribed conduct committed through the use of, or against, digital technologies. That definition says it all. It includes three areas of activity.

a. A crime committed against a computer, computer system, computer data or computer network [25]; Crimes in the commission of which computers are used. These include online fraud and financial crime, the electronic manipulation of share and other markets, the dissemination electronically of offensive material, misleading advertising, identity theft and so on.
b. Specific crimes committed against digital technology itself [26]. These would embrace hacking, cyber stalking, and theft of communication services and the transmission of malware viruses, worms, Trojans, botnets, backdoors, phishing and so on.
c. Conventional crimes attended by incidental cyber methods [27]. These might comprise encryption or steganography (the embedding of information in data) to conceal information relevant to other crime and the use of databases to store or organize information about criminal activity. Conventional crime is a social and economic incident and is as old as the human society. Conventional crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment. A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences. Put simply articles 3 to 7 of the proclamation no.958/2016 pertain to the following basic principles. These are the requirement of dishonest intent of perpetrators, public interest defense covering the accessing or intercepting of data for journalistic purposes and in the public interest; the offence should not be made out unless serious harm was done or likely to be done mainly for data interference and system interference offences; and the imposition of financial penalties as an alternative to imprisonment should be provided for in order to provide a proportionate penalty for minor infractions.

Under Article 8, it is an aggravating factor if any of the offences created in the preceding provisions pertaining to

[15], Ibid Article 2(1) (b) as it is stipulated in the proclamation that a conventional crime committed by means of a computer, computer system, computer data or computer network.
[16] Ibid Article 12
[17] Ibid, Computer crime proclamation no.958/2016,Article 11
[18] Ibid article 2(1)
[19] Ibid,Article 3
[20] Ibid,Article 4
[21] Ibid, Article 5
[22] Ibid Article 13.

[23] It has been adopted June 27, 2014, though not yet entered into force; at http://bit.ly/2achRPE Accessed 18 November 2017
[24] Ibid Article 25(3) Rights of citizens
[25] Ibid Article 2(1)(a)
[26] Ibid Article 2(1)(b)
[27] Ibid Article 2(1)(c)

computer system or data designated as top secret by the concerned body for is an aggravating factor if any of the offences created in the preceding military interest or international relation, and while the country is at a state of emergency or threat or whilst the country is at a state of emergency or threat, in this scenarios the corresponding reprimand shall be rigorous imprisonment from fifteen years to twenty five years [28]. Article 12 deals with the possessing or distributing child pornography, are in line with international human rights law, "Whosoever intentionally produces, transmits, sales, distributes, makes available or possesses without authorization any picture, poster, video or image through a computer system that depicts [29] Pornography on the net can take a variety of forms. It might comprise the hosting of web site containing these prohibited materials, Use of computers for producing these obscene materials. This may also include the downloading through the Internet, obscene materials. These obscene matters might cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

I argue that there is no clarity of erotic in Article 12(2). Hence, there may be a fear even that sending educational materials or content correlated to sexual health might be construed as erotic. Since enticing or soliciting is likewise vague this creates the danger of criminalizing sexual education or in the same way legitimate work. The drafting should be revisited to prevent this. The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason might be to prove them to be outstanding amongst other children in their group. As to me the proclamation article 12(2) should provide precise definition for terms like erotic, entice and solicit in order to assist pro-interpreters.

Article 19 establishes ambiguity by providing that diverse provisions can apply concurrently to offences, potentially setting different thresholds for liability, different defenses and different levels of punishment. As noted earlier, it is both needless and highly unwanted, in my aspect, to create specific online offences where an offline equivalent offence already exists under preceding articles 13 and 14 and it deems a redundant of those articles. This is particularly so given that online offences are generally punished more harshly than their offline equivalent contrary to international standards on freedom of expression [30]. At the very least, I argue that computer crime laws such as the Proclamation no 958/2016 ought to create confidence by providing either that they apply, as lex specialis or lex posterior, or that another law applies.

Last but not least I suggest for pro-legislatives continuing measurement of the extent of the problem and reviewing of its some provisions inconsistent in light of international human rights laws are indispensable. Solely against legislations can it be judged whether or not the investigation and prosecution of computer crime are being conducted could not solve the emerging problems efficiently.

C. Preventive and Investigative Measures

As proverb being uttered by many authors prevention is often better than cure. It is always better to take certain precaution whereas operating the net. Any individual should make the 5P tune for online security such as precaution, prevention, protection, preservation and perseverance. Article 21 of the proclamation inserted the principle of the prevention, investigation and evidence procedures provided in this Part and Part Four of this Proclamation shall be implemented and applied in a manner that ensure 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 [31]. The investigation of computer crime and the gathering of computer-based evidence encounter new problems. The expansion of data storage capacity has been mentioned. Even if investigators have a good idea of what they are looking for and a reasonable suspicion of where it might be, searches in digital memories might be hindered by the mislabeling of data, encryption, storage in secret directories or embedding in space that a simple file listing could disregard. I argue that data retention requirements should be reviewed in line with international standards on privacy and an independent body should oversee the implementation of the surveillance regime established under the Proclamation.

The problem might be encountered during as an evidence of a crime might be stored among other data that never relate to the investigation. Prima facie the data might be protected by privilege or privacy laws. Evidence of a crime being investigated may be stored with evidence that discloses other offending. If information about the former is being obtained according to a search warrant [32], evidence obtained about the latter may not be admissible in a prosecution. These can become real issues for prosecutors. The data under issue are in a networked system, the practical and impact problems that can arise from intervention by investigators can be serious.

Article 25 gives rise power for sudden searches to Attorney General may give permission to the investigatory organ to conduct interception or surveillance without court warrant where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure is or to be committed computer systems deemed to be at risk or at the source of an attack when there are reasonable grounds to believe that a computer crime is to be committed and it is necessary to prevent and control this, to provide early warning to citizens, or to minimize the risks for the effectiveness of an ongoing investigation. Article 26 provides that where there are reasonable grounds to believe that a computer crime is (being) committed, the police may arrest suspects, in accordance with the provisions of the Criminal Procedure Code. Article 27 imposes a duty on service providers to report the commission of the crimes stipulated in the Proclamation or dissemination of any illegal content data by third parties of which they have knowledge. They must also take appropriate measures, which are undefined. Another serious problem would happen when the digital evidence may be readily damaged or destroyed. For

[28] Ibid Article 8(a)(b)(c)
[29] Ibid Article 12(1)
[30] ACHPR/Res169(XLVIII)2010: Resolution on Repealing Criminal Defamation Laws in Africa P13
[31] Ibid Article 21.
[32] Ethiopia criminal procedure code (1961) article 25(2)

instance, an investigator on site might come across a system that is unusual and inadvertently destroy data. A computer may have been booby-trapped by the operator (perhaps by a short program that requires a password to be entered at intervals, failure of which triggers deletion), so that a search will trigger the destruction of data. A hot key may be programmed, destroying evidence when a particular key is pressed. When a police officer knocks at the door, the button may be easily pressed and evidence lost. In nutshell I want to convey hereby advanced skill and knowledge are entrusted to investigatory organs and continuing training for prosecutors in this arena is crucial. Prosecutors and national executing task forces need to have enough knowledge and understanding of the issues they are addressing in order to do so effectively [33].

D. Evidentiary and procedural provisions

Articles 29-37 provide for any computer data to be seized by order of court; and Article 31 provides rules on the admissibility of computer-related materials, such as printouts of emails, as evidence. Article 33 provides that the admissibility of Evidences person adducing evidence has the burden of proving its authenticity (for instance, than a print-out of an email is genuine), the obtaining and admissibility of evidence need to be considered. This is an arena where careful consideration needs to be given to the procedural law of the place of trial and the criminal procedural law of the places from which evidence is obtained. Is the admissibility of the digital evidence affected by the way in which it was obtained? Article 34 provides further detail on proving the authenticity of electronic documents. Article 35 ensures the originality of electronic documents which comprise any electronic record which is obtained upon proof of the authenticity of the electronic records system or by which the data was recorded or stored shall be presumed original electronic document. Article 36 deals with the presumption of courts when assessing the admissibility of evidence in accordance with this Proclamation, the court may have regard to the procedure, standard or manner in which a similar computer system is functioning. Article 37, in conclusion, provides that the burden of proof generally falls on the prosecution, but that, once fundamental facts have been established, the court may shift this burden to the defense. What are the appropriate punishments for this kind of offending? As information technology is used in the commission of an offence, does that make it more or less serious than a similar crime perpetrated by traditional means or does it make no distinction? How are the traditional purposes of punishment deterrence, retribution, reform, incapacitation measured against computer-offending? How many corporate offenders be implicated and punished? I argue that it is very essential having all these questions in mind ahead of rendering decision on suspected perpetrators.

E. Excutive organs of computer crimes

As it could be construed from the computer crime proclamation no. 958/2016 the subject of computer crimes might be categorized into groups such as crime against Individuals (i.e. their person, and their property of an individual), crime against organization (i.e. government, and firm, company, group of Individuals), and crime against Society at large. In order to safeguard aforementioned targets of computer crimes articles 38 through 41 provide the institutions empowered to follow up the cases of computer crimes in Ethiopia. They comprise public attorney general, prosecutors, national executing task forces and police department. It is very interesting provision stipulated under article41(3) is the Task Force shall, for the prevention and control computer crimes, develop national discussion forum, discuss on occasional dangers materialized and provide recommendation thereof, design short and long-term plans to be performed by the respective institutions as well as put in place synchronized system by coordinating various relevant organs [34]. Article 40 is dealing with the jurisdiction in which a prosecution should be brought that Federal high court, once an offender has been detected. The potential problem is electronic impulses could cross many jurisdictional boundaries before hitting their targets or bringing about the responses they seek. A computer perpetrator can sit in one country, route electronic communications through several others, commit a crime in another and park the proceeds in yet another. Crimes could be perpetrated in several countries along the way. Decisions may have to be made about where the criminal might be amenable to justice and what crimes ought to be prosecuted, under what law (and where) in the general public interest. Practical implications such as the effective obtaining of evidence may impact on those decisions.

F. Miscellaneous Provisions

These provisions remind the importance of international cooperation in order to halt the computer crimes. The Federal Attorney General shall cooperate or enter in to an agreement with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, and extradition and other assistances in pursuance to this Proclamation and agreements to which Ethiopia is a party and within the limits of the country's legal system [35]. This provision sheds a light on the issue of national law vis-à-vis international law and jurisdiction in computer crime. It also covers the concepts of prescriptive, enforcement, territorial and extra-territorial jurisdiction in the cases of cyber crimes. In addition, a deep insight has been made into the question whether computer crimes are extraditable offences?

4. Conclusion and Suggestion

An attempt has been made to point out the shortcomings and lacunae in the computer crime proclamation no.958/2016 and to suggest remedial measures to ensure effective prevention and control of the computer crimes. Capacity of human mind is profound. It is impossible to get rid of computer crime from the computer space. It is quite feasible to check them. History is the witness that no legislation has thrived in entirely avoiding computer crime from the sphere. The solely plausible step is to make people aware of their rights and duties (to

[33] See, Ibid Computer crime proclamation no.958/ 2016, Articles 23 through 41.

[34] Ibid, Article 41(3)

[35] Ibid Article 42(1)

report crime as a collective duty towards the society) and more making the application of the laws more stringent to check crime. Undeniably the computer crime proclamation 2016 is a historical step in Ethiopia. Moreover I suggest that there is a need to bring changes in the Information communication Technology (ICT) to make it more successful to combat computer crime. I would sum up with a word of caution for the pro-legislatives (HPR) that it should be kept in mind that the provisions of the computer law are not made so stringent that it may retard constitutionally guaranteed human and democratic rights of citizens especially right to privacy and freedom of expression and prove to be counter-productive

5. References

1. United Nations Universal Declaration of Human Rights, 10, December, 1948.
2. United Nations General Assembly Resolution 217A (III), adopted, 1948.
3. United Nations International convention on civil and political rights, 1966.
4. African (Banjul) charter on human and peoples' rights, Adopted 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force 21 October 1986
5. Constitution of the Federal Democratic republic of Ethiopia, proclamation no.1/1995
6. The Criminal Code of the Federal Democratic Republic of Ethiopia proclamation no.414/2004
7. Ethiopia computer crime proclamation No.958/2016