ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 3, Issue 1, pp: (92-104), Month: January - March 2015, Available at: www.researchpublish.com

Computer Crimes in Ethiopia: An Appraisal of the Legal Framework

Molalign Asmare

LLB, LLM, Lecturer at Wolaita Sodo University, School of Law

Abstract: **The rapid technology of computer and networking plays a prominent role for the rapid global development. However, innovations of computer technologies, in addition to help and faster development, became the target and the instrument for the commission of crime. Currently, computer crimes are the newly emerging and rapidly growing crime. The global nature of computer crime or cybercrime creates a major challenge for national criminal justice systems. Thus, in combating computer crimes, various measures have been taken at the international, regional and national level. At the national level, many countries in the world respond to by enacting new criminal legislations including Ethiopia. Ethiopia amended and replaced the 1957 Penal Code by the 2004 Criminal Code. One of, inter alia, justifications to enact the 2004 Criminal Code is to address crime born of advances in technology such as computer crime. The 2009 ICT Policy and the 2011 Criminal Justice Policy of Ethiopia also reveal the great attention given to computer crimes. However, the 2004 Criminal Code of Ethiopia composed of only six articles (Articles706-711) under the scheme of 'property crime'. Under these provision, accessing; accession and taking or using data; accessing and deleting or altering; or denial of services on computers, computer system, computer networking intentionally or negligently, constitute computer crime. This research tries to critically analyze how the Ethiopian Criminal Code criminalizes computer abuses according to its unique nature and to what extent the legislative measures are importantly proportional to the prevalence of such crime. Considering the nature, type, impact, and targets of computer crimes and criminals, this research, concluded that computer abuses did not carefully and sufficiently criminalized according to their unique nature, impacts, and the provided punishments are disproportionally lenient,**

Keywords: **computer crime, nature of computer crime, impacts of computer crime, combating computer crime, the 2004 Criminal Code, principle of proportionality, punishment.**

1. COMPUTER CRIME: GENERAL OVERVIEW

1.1. Introduction:

The rapid technology advancement of computer and networking plays a prominent role for rapid global development.[1] Such developments in modern technology have great contributions for countries development and expansion through communication networks, faster and easier networking and information exchange.[2] However, innovation of computer technologies, in addition to help and fasten development, becomes the target and the instrument for the commission of crimes.

In the contemporary world, computer crimes are the newly emerging and rapidly growing crime. As businesses and societies in general increasingly rely on computers and internet-based networking, computer crime and digital attack incidents have increased around the world.[3] One of the most and the highest dangerous risk of computer crime, *inter alia*, is the increased threat to national security. It is because of many modern critical infrastructures, such as, air traffic control

[1] Charlotte Decker, *Cyber Crime*: *An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, South California L.R. Vol. 81:959, 2008, at 959.
[2] See *Cyber Crime a Growing Challenge for Governments*, KPMG International, Swiss, 2011, at p.2.
[3] *Id*.

system, the electric power grid, telecommunication network, financial sectors, and critical governments' services like national defense, are dependent upon networked computing which is vulnerable to computer crime.[4] Usually, computer crimes are common in its commission by targeting persons (against persons), business and non-business organizations (against property), governments (against the state) and the society (against morality) on the confidentiality, integrity and availability of computer data and system.[5] This situation obliged countries to take different legal measures, even as to the extent of amendment of their criminal laws, including Ethiopia.

This research addresses central questions how the Ethiopian Criminal Code criminalize computer crimes according to its unique nature? And to what extent the legislative measures are importantly proportional to the prevalence of such crime? To address these issues, this paper will try discus the general notion of computer and internet crime, their type, impact and nature; and an evaluation of the Ethiopian legal framework in general and the Ethiopian Criminal Code in particular. Furthermore, for the sake of clarity and illustration, it deals with the policy aspects and existing substantive criminal law of selected countries that address this technology dependent crime.

1.2. Computer Crimes: Defined:

Although there is no universally accepted definition of computer crimes,[6] the terms "cybercrime", "computer crime", "information technology crime", "high-tech crime", "e-crime", and "electronic crime" are usually used interchangeably to denote two major categories of offences i.e. computer or cybercrimes or and computer-related crimes. Cybercrime consists of two categories: computer related crimes and computer crimes.[7] So there is broader and narrower kind of definitions about cyber crime or computer crime in order to conceptualize what it is. However, some scholars argued that defining the term either too broadly or too narrowly creates unintended problem. If we define both too broadly, then we risk creating a threat that never appears or defining the terms too narrowly will have the chance missing the real problem when it comes.[8] Other legal scholars have argued that a broad definition of the term is necessary because of the diversity and rapid emergence of new technology-specific criminal behaviors.[9] For example, the United States Department of Justice defined computer crime broadly as: *"any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution."*[10] The 2001 Communication of the Commission of European Union defined computer-related crime in abroad senses as: *"any crime that in some way or the other involves the use of information technology."*[11] The Council of European Convention on Cybercrime of 2001 defines cyber crimes in four different categories i.e. offences against the confidentiality, integrity and availability of computer data system; offences of computer-related; offences of content-related; and offences of copy right-related.[12]

Whereas under the 2004 Ethiopian Criminal Code no one can find a direct specific definition provided for the term computer crime. Rather the prohibited acts on and through computer are listed under Article 706-711 of the Code. However, it does not mean that one cannot draw the definition from the cumulative reading of Article 23,[13] which stated what a crime constitute, together with Articles that deals with computer crime under the Code.

Generally, computer crime or cyber crime is a term used to broadly describe a criminal activity in which computers or computer networks are a tool, a target or a place of criminal activity and include everything from electronic cracking to

[4] Decker, *supra* note 1, at 961-962.
[5] Marco Grercke, *Understanding Cyber Crime: Phenomena, Challenges and Legal Res*ponses, ITU Publication, 2012, at11.
[6] Yasin Aslan, *Global Nature of Computer Crimes and the Convention on Cybercrime*, Ankara L.R, Vol.III No.2, 2006, at 3.
[7] Sylvia Mercado Kierkegaard, *Cracking down on Cybercrime Global Response: the Cybercrime Convention*, Communication of the IIMA, Vol.V. Issue No.1, 2005, at 60.
[8] Carl J. Franklin, *The Investigator's Guide to Computer Crime*, CHARLES C. THOMAS-PUBLISHER, LTD. Illinois, U.S.A.,2006, at7.
[9] Rizgar Mohammed Kadir, *The Scope and the Nature of Computer Crime Statutes: A Comparative Study*, German L.J., Vol. 11 No.06, 2010, at 614.
[10] Mike Keyser, *The Council of Europe Convention on Cybercrime*, J. Transitional Law and Policy, Vol. 12:2, 2003, at 290.
[11] Laura Ani, *Cybercrimes and National Security: The Role of the Penal and Procedural Law*, Law and Security in Nigeria, 2011, at 199.
[12] See Council of European Convention on Cybercrime, ETS 185, 23.XI, Budapest, (2001).
[13]See the Criminal Code of the Federal Democratic Republic of Ethiopia, *Negarit Gazzeta*, Proclamation No.414/2004, 9th of May, 2005, (hereafter the criminal code) Article 23 of the Criminal Code defines crimes as: (1) A crime is an act which is prohibited and made punishable by law. In this Code, an act consists of the, commission of what is prohibited or the omission of what is prescribed by law. (2) A crime is only completed when all its legal, material and moral ingredients are present.
(3) Notwithstanding the provision of sub-article (2) of this Article, a juridical person shall be criminally liable to punishment under the conditions laid down in Article 34 of this Code.

denial of service attacks.[14] In other words, computer crime or cyber crime is an activity involving the information technology infrastructure, including illegal access, illegal interception, data interferences, system interferences, forgery (identity theft) and electronic fraud[15] without including the physical harm inflicted to the computer hard body.[16]

1.3. Nature of Computer Crimes:

Computer or cyber crimes have some unique nature that one cannot find in other forms of traditional crimes. The incidence of traditional crime, mostly, is easy to deal by the law enforcement agents. In such a type of crime, the location where the crime is committed can be traced out; individuals that involved in such a distinct incidence can be identified; facts and issues can be investigated; and liabilities can be imposed.[17]

While cyber or computer crime is not a distinct type of crime like traditional crimes such as rape and murder. It denotes the use of technology and higher technical skill to commit crimes. Computer crime is not a kind of real-world crime in which the victim and the offender relatively have a closer physical proximity when the crime is committed. It is rather the victim's computer, the intervening computer, and the computer servers (network) are used to the commission for a computer crime. Computer crime is not limited to a certain jurisdiction rather it is a borderless crime.[18] This global nature of computer crime or cyber crime constitutes a major challenge for national criminal justice systems and their jurisdictions[19] because of the criminals are located in different countries and they can target huge number of victims at once throughout the world.[20] In other words, like other real-world criminal activities, the computer criminality is not limited to any specific type or any particular region or any particular target group.[21] Cyber crime or computer crime is easy to commit for the one who has know how; hard to detect for the one who has a know how to erase one's tracks; and usually hard to locate in jurisdictional terms.[22]

As a matter of fact, any internet user may become the victim of computer crime. However, such victimization is not limited only to those who are computer user, but it does also affect anyone living in anywhere in the globe.[23] Such kind of victimization, for example, may appear where the computer criminal (computer hacker) changes the medical prescriptions stored in a certain hospital's computer memory.[24] Generally, the nature of cybercrime or computer crime is highly complex, self-reinforcing, technologically advanced, geographically widespread and indiscriminate when we examine it with regard to the tools, nature, perpetrators and the victims.

1.4. Types of Computer Crime:

Determining the types of condemned activities related to the computer is crucial because the quality of their legislative treatment can be as good as the original determination and classification of such activities.[25] Abuses or crimes related to computers take different and various forms. They are, however, classified in several ways according to more than one criterion.[26] One approach can be found in the European Convention on Cybercrime, which distinguishes four different types of offences i.e. offences against the confidentiality, integrity and availability of computer data system; computer-related offences; content-related offences; and copy right-related offences.[27] The second classification of computer crimes

[14] B. Muthukumaran, *Cybercrimes Scenario in India*, Criminal Investigation Department Review, 2008, at 17.
[15] Ani, *supra* note 11, at 201.
[16] Vijaykumar S. Chowbe, *The Concept of Cybercrime: Nature and Scope*, Global Journal of Enterprise Information System, Vol. 3, Issue-1, 2011, at 75.
[17] *Id*.
[18] *Id*, at 132.
[19] Joachim Vogel, *Towards a Global Convention against Cybercrime*, First World Conference on Penal law in Guadalajara, Mexico, 2007, at 2.
[20] See Cybercrime Strategy, *The Secretary of the State Presentation to the Parliament*, Crown Publication, U.K., 2010, at 10.
[21] Pramond kr. Singh, *Laws on Cybercrimes*, Book Enclave, India, 2007, at 9.
[22] Ani, *supra* note 11, at132.
[23] Singh, *supra* note 20.
[24] *Id.*
[25] Kedir, *supra* note 9, at 615.
[26] *Id.*
[27] See the European Convention on Cybercrime, *supra* note 12. Offenses against the confidentiality, integrity and availability computer data system- a type of crime which includes illegal access and interception o f data; data and system interference; and misuse of devices (stated from Article 2-6); computer-related offenses- a type of computer crime which comprises computer-related forgery and fraud (Article 7-8); content related offenses- A crime or an offence which typically related to child pornography (Article 9); and copy right-related offenses-offences related to copy right and intellectual property right (Article 10).

makes use of two categories.[28] These are: types of crimes where a computer system itself is the target such as hacking; viruses, worms, Trojan horse, logic bombs, and sniffers; denial of service attacks; and cyber terrorism (the so-called computer related crimes); and traditional crimes like fraud and theft, and child pornography that are facilitated and enabled by the computer (the so-called computer-enabled crimes).[29]

Another typology of computer crimes is the system adopted by the United States Department of Justice. This system separates computer crimes into three categories based on the computer's role in a particular crime. In such classification, computer may be the 'object', 'subject', and 'instrument' of crimes.[30] Computer, as the 'object' of crime, happens where the criminal commits an attack up on an individual computer or a network and such attack may include unauthorized access to information on the computer or the targeted network; unauthorized corruption of information; or theft of an electronic identity.[31] Secondly, computer as the 'subject' of crime is a situation where the computer is become the physical site of a crime, or a source, or reason for unique forms of asset loss. Hacking, and disseminating of Viruses, Worms, Logic Bombs, and Trojan Horses are some of the most common types of computer crime when a computer is the subject of crime.[32] Finally, a computer could be the instrument for committing traditional offences such as to steal credit card information, store and distribute obscenity, or distribute child pornography and other types of obscene materials via computer linked to internet.[33] When we see the contents of offenses stated under the Ethiopian Criminal Code, even though they are not comprehensive enough, the Ethiopian typology of computer crimes are almost similar to the typology of the United Sates Department of Justice typology.

There are also literatures that tried to classified computer crimes into three in a more similarity, but a bit difference with the classification of U.S. Department of Justice. Thus, computer crimes can be divided into three general categories, namely, crimes where a computer is the target, crimes where a computer is a tool, and crimes where a computer is incidental or container.[34] The first two types of computer crimes are similar with the U.S. Department of Justice. What this typology makes differ is the last one which deals about a crime where a computer is incidental to the crime. A computer is incidental to the crime if the computer itself is not require for the crime but, is used in some way connected to the criminal activity such as a threatening letter that was written and stored in the computer; financial records on a drug dealer machine; and the like.[35]

1.5. Targets of Criminals:

Computer criminals can vary in terms of both age and skill level so that their target varies accordingly.[36] Computer criminals can be teenage hackers, annoyed employees and company insiders, or international terrorists and spies.[37] Sometimes, the targets of computer criminal may differ according to their motives to engage in such crime.[38] Some scholars identified a lot of possible motives for committing computer related crimes whether a computer is subject or object of crime. These are: "to exhibit technical prowess"; "to highlight vulnerabilities in computer security systems"; "to punish or retaliate"; "to engage in computer voyeurism"; "to assert a philosophy of open access to computer system"; and "to sabotage"[39] From these, one can note that there are some criminals who have identified target whereas other have not. Therefore, the targets of computer criminal are different according to their typology. As it is stated hereinbefore under nature and types if computer crime section, the target of computer criminals can be data, networks or access that that harm individual, institutions and the governments. It includes financial institutions, military infrastructures, states' classified information, banks, hospitals, private data or information, court and police recordings, trade secrets and the like. The other the calls the attention of computer criminals is the weakness of criminal law. Countries which has no or weak criminal

[28] Singh, *supra* note 20.
[29] Aslan, *supra* note 6, at 133.
[30] Kedir, *supra* note 9, at 616.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] Marc D. Goodman, *Why the Police Don't Care about Computer Crime*, Harvard Journal of Law and Technology, Vol.10, No.3, 1997, at 468-469.
[35] *Id.*
[36] Kadir, *supra* note 9, at 617.
[37] Vogel, *supra* note 19.
[38] Kadir, *supra* note 9.
[39] *Id.*

law with respect to computer crimes or cybercrimes is the targets of computer criminal than those countries which has strong computer criminal law.[40]

1.6. Impacts of Computer Crimes:

Computer crimes or cybercrimes have various impacts on the national security of a given state, economy, privacy, public morals, and on life.

The highest and the most impact of computer crime rests upon the national security of a given state.[41] Due to the fact that highly modern and critical infrastructures such as air traffic control system, electric power grid, telecommunication networks, the financial sectors; and critical government services such as emergency and national defense services, are highly dependent on networked computers. Thus, they are highly affected by computer crimes.[42] Moreover, states classified information that may affect the national interest of a country may subject to attack. Secondly, computer crimes costs the global economy in billions of dollars each year, which translates into loss of jobs, lost of taxes, lost innovations, higher costs for the consumers, lost of confidence in electronic or internet commerce, and stunned global trade.[43] Thirdly, when computer crimes become the prevalence, the collection, storage, transmission, and connection of personal data endangered the personality rights of citizens.[44] The clear infringement of computer crimes on privacy is highly affected traditionally protected professional secrets, especially official secrecy and the requirements of confidentiality for officials, doctors, lawyers, banks and the like.[45] Similar impacts occurred with respect to the storage of user data i.e. the data that is required for purpose of billing, statistics, and criminal investigations and with respect to computer networks i.e. the data transferred in international computer networks aggravate the risk of violation of privacy.[46] Fourthly, computer crimes or cybercrimes has adverse impacts on public morals by disseminating illegal and harmful contents.[47] Computer crimes are instruments and places of distributing illegal and immoral information. Be it glorification of violence, religious offences, racism, nazism, and hate speech, are much more effectively disseminated or distributed by means of electronic communication in international networks.[48] Finally, computer manipulations do not only serve to the purpose of gaining pecuniary benefits, violations of the right to privacy of the authorized user, and distributing harmful and immoral contents, but also used for attacks on human life, for example, the manipulations of a flight control system or a hospital computer.[49]

2. COMBATING COMPUTER CRIMES

2.1. Introduction:

In combating computer or cyber crimes, various initiatives have been taken at the international, regional and national level. In international level, a number of international organizations work constantly to analyze the emergence of cybercrime and to develop strategies in combating computer or cybercrime.[50] The main actors for these initiatives are: the Group of Eight (G8); the United Nations and United Nations Office on Drugs and Crimes; the International Telecommunication Union; and the International Criminal Police Organization.

In addition to the international organization, there are many regional organizations that focus on specific region with regard to the activities that deal with issues related to combating cybercrime. These regional organizations are mainly: the Council of Europe, European Union, Asia-Pacific Economic Cooperation, African Union, Arab-League and Gulf Cooperation Council, and the Organization of American States. At the national level, given due concern as to the threat of computer crime, many countries in the world responded to by enacting new criminal legislation and many others are on

[40] Singh, *supra* note 20.
[41] Decker, *supra* note 1.
[42] *Id.*
[43] *Id.*
[44] Ulrich Sieber, *Legal Aspects of Computer-Related Crime In the Information Society*, COMCRIME-Study, Prepared for the European Commission, Version 1.0, 1998, at 38.
[45] *Id*, at 39.
[46] *Id.*
[47] *Id*, at 54.
[48] *Id*, at 54-55.
[49] *Id*, at 57.
[50] Ani, *supra* note 11, at 114.

the way to take similar legislative steps. For the sake of this research, the majority of issues concerning national approach regarding computer crimes deal with the Ethiopian legal framework.

2.2. Computer Crimes in Ethiopia: An Appraisal of the Legal Framework:

2.2.1. Criminalizing Computer Misuse or Abuse:

Due to the prevalence of computer cyber crimes throughout the world, many countries have been amending the existing penal code or in the way of enacting the new one so as to address computer related crimes with its specific scope and nature. Ethiopia, for example, has amended and replaced the existing Peal Code of 1957 by 2004 Criminal Code. The basic justification to come up with the 2004 Criminal Code is to amend or add provisions that require changes, clarity or to fill the gaps in the new emerging criminal behaviors after the Penal Code has come into force.[51] The clearly indicated justification for the adoption of the new Criminal Code under its preamble is to address crimes born of advances in technology. Other countries such as United States, Japan, China, India and others have been enacted and amended their laws for similar objectives.

The United States Computer Fraud and Abuse Act of 1984, for instance, identify and outlaws seven specific activities involved with the unauthorized access, reproduction, and destruction of electronic data.[52] This Act is the first comprehensive cyber-crime act in USA Federal law, and it stands as a part and parcel of the American Criminal Code.[53] Similarly, the Indian Information Technology Act of 2000 specifically deals with unauthorized access, unauthorized downloading, virus attacks or any containment, causes damage, disruption, denial of access, interference with service availed by a person.[54] In the People's Republic of China, computer-related crime covered by Article 285-287 of the Criminal Code.[55] The Japanese Unauthorized Computer Access Law of 2003also criminalized the act of unauthorized computer access in which another's identification code or password is stolen, and security hole related attacks.[56]

Obviously, the main sources of the provisions of computer crimes in the Criminal Code are USA laws (Massachusetts Law: 'An Act to Prevent Computer Crimes of 1990'; Texas Law: 'Computer Crime Law 1994; USA Federal law: 'Fraud and Related Activities in Connection with Computers'; and Michigan State University writings on 'Computer Crime: An Emerging Challenge for Law Enforcement 1997') and the English Computer Misuse Act of 1990.[57] The 2004 Criminal Code of Ethiopian is composed of only six articles (Article 706-711) under the scheme of 'property crime' of Criminal Code which deals about computer crime. Generally, under those provisions: accessing, accessing and taking or using data; accessing and deleting or altering; or denial of service on computers, computer system or a computer network intentionally or negligently is an act of computer crime.

Moreover, Ethiopia has come up with the National Information and Communication Technology Policy and Strategy in 2009 (ICT Policy) and Criminal Justice Policy of 2011. The ICT Policy's the main objectives are: to address the national security implications arising from widespread application of ICT within the economy and the society; to secure and safeguard the national electric communication system (national, institutional and individual security) and protect both data and network integrity; and to prevent, detect and respond to cyber crime and abuse of ICT so as to contribute to the fight against national, regional and international crimes.[58] Under this Policy, the Ethiopian Government seems highly appreciate the nature and impacts of the ICT abuse such as computer crimes or cyber crimes on the national, institutional and individual security of data, network and the like.[59]

Additionally, Ethiopia has adopted the new Criminal Justice Administration Policy in 2011with new approach.[60] The full implementation of this new Policy requires many changes and additions to the existing law, in particular the criminal

[51] Elias N. Stebek, *Principles of Ethiopian Criminal Law*, St. Marry University College and USAID, Addis Ababa, 2013, at.22.
[52] Ryan Handerhan, *Japan and American Computer Crime Policy*, Dietrich College Honors Thesis, Paper 69, 2010, at 6.
[53] *Id.*
[54] Kamini Dashora, *Cyber Crime in the Society*: Problems and Preventions, Journal of Alternative Perspectives in the Social Sciences, Vol.3, No.1, 2011, at 253.
[55] Tonya L. Putnam et al, *International Responses to Cyber Crime, Hoover Press*, DPsHPCYBE02006-25: Rev.1, at 43.
[56] Handerhan, *supra* note 52, at 17.
[57] See the Drafting Committee's Elaboration on the Provisions of the Federal Democratic Republic of Ethiopian Criminal Code, at 321.
[58] See the Ethiopia National Information and Communication Technology Policy and Strategy, (2009). (Hereafter the ICT Policy).
[59] *Id.*
[60] See the Federal Democratic Republic of Ethiopian Criminal Justice Administration Policy, Ministry of Justice, (2011). (Hereafter the Criminal Justice Policy).

code, the criminal procedure code, and existing law concerning criminal evidence. In addition to the main changes explicitly required by the new policy, it has a great concern about computer and cyber crimes.[61] The policy has given a due attention for the prevalence of computer and internet crimes. As it is clearly stipulated under the policy, one of among the very purposes of the policy are securing the government and the society from computer crimes and to prevent computer crimes proactively and take appropriate measures if once committed.

The policy, as computer crime is concerned, stated the measures that are to be done: these are mainly, when the national crime prevention strategy is formulated, it should encompass details about computer and internet crimes; to integrate both governmental and non-governmental with a view to protect themselves from incidences of computer crime; to have international cooperation guidelines; and capacity building training for law enforcement agencies.[62] Like the ICT Policy, the Criminal Justice Policy also reveals the great attentions given to the computer crimes than the 2004 Ethiopian Criminal Code.

2.2.2. Computer Crime under the Ethiopian Criminal Code:

The 2004 Federal Democratic Republic of Ethiopian Criminal Code incorporates most of the provisions of the 1957 Penal Code with some amendments or additions to the provisions that require changes, clarity or gaps in the new emerging criminal behaviors after the Penal Code has come into force.[63] The Criminal Code has incorporated new provisions required by the current realities that have outspread since the promulgation of the former penal code.[64] The clearly indicated justification for the adoption of the new Criminal Code under its preamble is to address crimes born of advances in technology. One of the admirable works of the Ethiopian legislature is criminalizing acts of computer abuses, though it has its own pitfalls. Computer crimes as one of among other justifications to adopt the new Criminal Code and computer crime as a "crime" in general and as a "property crime" in particular will be discussed in the next subsections.

2.2.2.1. Computer Crime as "Justification" of New Criminal Code:

The Ethiopian Criminal Code has been enacted with a lot of justifications. As it is stated in the preamble, after the coming into force of the 1957 Penal Code, radical political, economic, and social changes that are out of the scope of such Penal Code have taken place. The recognition of equality between religions; nations, nationalities, and peoples; the need for protection and promotion of human rights and democratic rights by the Federal Democratic Republic of Ethiopian Constitution and International agreements ratified by Ethiopia can be cited as an example.

The other, but the main concern of this paper, justification proposed by the Ethiopian Legislature to adopt a new Criminal Code is the lacunae the 1957 Penal Code to address properly the subsequent and technology dependent crimes. The major crimes born of advance in technology and complexities of modern life are hijacking of aircraft, computer crimes, and money laundering. Thus, one can confidently argue that computer crimes were not prevalence at the time of drafting the 1957 Penal Code and thereby it is not treated as a crime. Whereas, in the new Criminal Code, computer crime is not only an act prohibited by the law but also the core justification for the Ethiopian Legislature to come up with the 2004 Criminal Code. Since the new Criminal Code is intended to criminalize computer abuses as one of the major justification to come up with such new code, the legislature should have carefully and clearly stated those provisions that are required to criminalize those computer abuses according to their nature, impacts; and establish proportional punishments that fit with such crime.

One might expect more treatments of computer crime who only read the preamble of the Criminal Code, and therefore, whether computer crime is treated equivalent to its nature and impacts on the state national security, public morality, individual privacy, country's economy, on health, life etc… is in question.

2.2.2.2. Computer Crime as a "Crime":

Crime, under the legalistic definition, denotes those behaviors that are formally prohibited and punishable under criminal law.[65] In other words, it is the commission of an act that violates a criminal code enacted by an officially constituted

[61] See Preliminary Analysis of the Legislation Requirements of the Criminal Justice of the Criminal Justice Administration policy, Federal Democratic Republic of Ethiopia, 2009, at 1.
[62] *Id*, at 45.
[63] Elias, supra note 51, at 22.
[64] *Id*.
[65] Martin O'Brien and Majid Yar, *Criminology: The Key Concepts*, Routledge Press, London, 2008, at 32.

political authority. Crime is also the omission of a duty that makes the offender liable to punishment by law, or behavior that is prohibited, as well as behavior or an act that is required by law. The Ethiopian Criminal Code defines crime as: "An act of commission or omission which is prohibited and made punishable by law".[66]

The researcher has a great appreciation to the legislature to come up with the criminal law that criminalizes computer crime. However, there are only few provisions that deal with computer crime. The prohibited behaviors or acts by these provisions are intentional or negligent accessing a computer, computer system or computer network without authorization (here is only accessing is a prohibited act or it amounts to crime)[67]; accessing a computer, computer system or computer network, and taking, using or causing to be used data or computer services (here accessing plus taking, using or causing to be used the computer data, system or network is prohibited)[68]; accessing a computer, computer system, or computer network and causes damage by adding, altering, deleting or destroying data (accessing and damaging is a criminal act, and computer is a target to criminal act)[69]; accessing and adding, altering, deleting, or destroying a computer data or services to steal, defraud, deceive or extort or wrongfully control to obtain money or property is amounts to computer crime (here computer is an object to the crime)[70]; accessing of a computer, computer system, or computer network and disrupts the use of the computer by an authorized user (denial of services) is a computer crime[71]; and acts committed to further the commission of one of the acts specified in the preceding articles (Article 706-708), imports, produces, sells, offer for sale, distributes, buys, receives, or possesses instruments, secret codes, or passwords is a prohibited act in the Criminal Code.[72]

The other issue that will attract the attention of readers is Article 710 of the Criminal Code. The Article stated as *"Where one of the other crimes provided under this Code is committed by means of a computer, the relevant provision shall apply."* In the provision, the phrase "other crimes", has the idea of other real-world crimes which are prohibited by the Criminal Code, for instance, theft (acts against property), hate speech or racism (acts against honor or dignity), homicide (acts against life), and the like, and such acts are committed by "means of" a computer (here computer is the object or instrument to commit other crimes). In such cases, the relevant provisions stated elsewhere in the Code shall apply. It is difficult, however, to believe that the legislature had either thoroughly aware or given due concern to other incidents of computer crime on life, public morals, national interest, and privacy. Because it is safe to argue that, had the legislature given the due attention for other crimes with property crimes, it would not simply skip over without having full-fledged Criminal Code that appropriately address all possible impacts of computer crimes.

Finally, the last article which deals about concurrence of crimes is Article 711. The article stipulated that *"Where any crime committed by means of computer, has resulted in the commission of another crime punishable under this Code, the relevant provision shall apply concurrently."*

Crimes under the Criminal Code are categorized mainly as crimes against the interest of the state, against the interest of the community, and against individuals and family (including crimes against property). Are those crimes only concurrent to other property crimes? Or any other crime? If the answer it negative, it can highly affect the legislature justification to characterized computer crime only under property crime. If the answer is positive, it questions the legislature why it did not dare to have self-sufficient computer crime law that is only related to property crime.

Therefore, the provided provisions under the Criminal Code are not sufficient to address the nature of computer crimes. By having these stand alone six provisions, it is fair to argue that computer crime is not treated as its nature, impact, and necessitated to adopt such Criminal Code.

2.2.2.3. Computer Crime as a "Property Crime":

The Criminal Code of Ethiopia has three parts and each part has different books. For example, part one is the general part and has two books i.e. book I and book II, which deals about 'Crime and Criminal' and "Criminal Punishment and its Applications" respectively. In addition, Part Two, which is called the 'Special Part', consists of four books. To mention it, book III deals about 'Crimes against the State or National Interest or International Interest"; book IV embodies "Crime

[66] See the Criminal Code, *supra* note 13, Art. 23.
[67] *Id*, Art. 706(1).
[68] *Id*, Art. 706(2).
[69] *Id*, Art. 707(1).
[70] *Id*, Art. 707(2).
[71] *Id*, Art. 708(1).
[72] *Id*, Art. 709.

against Public Interest or the Community"; book V comprises "Crime against Individuals and the Family"; and book VI about "Crimes against Property". Finally, Part Three incorporates the "Codes of Petty Offences". [73]

The Criminal Code characterized computer crimes under the scheme of crimes against property. Thus, one first should note the classification of "property" and "crimes" under the Ethiopian Legal System. Under the property law of Ethiopia, especially under the 1960 Civil Code, goods have been classified into corporeal and incorporeal. Corporeal goods are further divided into movables and immovable. This kind of classification can be termed as the primary classification of goods (classification based on mobility). Other classification such as consumable and non-consumable, fungible and non-fungible etc. can be termed as secondary classification (subsidiary of complementary) classification of goods.[74]

Thus, the property crimes under the Criminal Code, the schematization of crimes against property under Book VI of the Code have a separate treatment of "crimes against property"; "crimes against rights in property"; and "economic and commercial crimes". Crimes against property comprises like crimes against movable property such as theft, robbery, looting, piracy etc; crimes against immovable property such as damages to herds, flocks or disturbance of possession or holdings etc; and damage to property. Moreover, "crimes against the right in property" includes crimes involving fraud; computer crimes; and crimes that involve moral or material intimidations. And finally, economic and commercial crimes consists of crimes against intangible rights such as attacks on another's credit; harmful false information; infringement of marks, designs, or models, or infringement of rights relating to literary, or artistic, or creative works; and crimes relating to proceedings of debt, execution and bankruptcy.[75] The categorization of computer crimes under "crimes against the rights in property" seems the Criminal Code treats computer crime as a crime against incorporeal property. Assessing all the above mentioned types of property crime is out of the scope of this research paper. The researcher rather concerned about the characterization of computer crime under such limited category.

Classification of crimes or offences differs jurisdiction to jurisdiction. In some jurisdiction, crimes can be classified based on legal element, material element, and mental element.[76] The other types of crime dichotomy is based in their nature i.e. *mala in se* and *mala prohibita*.[77] Others classified crimes into indictable offences (offences which are the most serious) and summary offences (minor offences).[78] There are also others which classified crimes based on their degree and quantity of punishment i.e. treason, felonies and misdemeanor.[79] Generally, offences may be classified based on the seriousness of crimes or on the subject matter of the crime. The Criminal Code is highly inclined to classify crimes based on the subject matter of crimes as one can easily note from the schematization of crimes. It classified crimes based on the types of interest to be protected by the law i.e. to protect the interest of the state, the community, and individuals (includes life, body, liberty, honor, moral, family, and property, etc).

Therefore, as we have seen it before, the nature and impacts of computer crime, its global and dynamic nature widens the scope of the victims and types of crimes that affects different interests. Computer crimes cannot only be construed as property crime as it can affects the political, economical and security interest of the state very seriously. Computer crime can affect the community at large very seriously. It can be the effective instrument to attack the public morals in an

[73] See the Criminal Code, *supra* note 13.
[74] Murado Abdo, *Subsidiary Classification of Goods under Ethiopian Property Law: A Commentary*, MIZAN LAW REVIEW, Vol.2 No.1, 2008, at 52-54. "The division of goods into corporeal and incorporeal is one of the multitudes of subsidiary classification recognized in the property law of Ethiopia. A corporeal thing is any product a human person can perceive whereas an incorporeal thing is any product that human beings cannot perceive, but which has economic value. Incorporeal things are rights of property that can only be claimed or enforced by legal actions and not by taking physical possession such as bank accounts, shares, trademarks, trade secrets, and copy rights". *id*.
[75] Ibid.
[76] See *An Introduction to the Criminal Law of Afghanistan*, ALEP, (2009), at 34.
[77] Joycelyn M. Pollock, *Criminal Law*, Matthew Bender & Company, Inc, 9th ed.,2009, at 19. "Mala in se: these are acts that are immoral or wrong in themselves, or acts that are naturally evil. *Mala in se* crimes are considered wrong in any society and include the common law crimes of murder, rape, arson, burglary, and larceny. Mala prohibita: these crimes are not naturally evil, but are prohibited by statute because they infringe upon the rights of others. This type of act is not wrong in some societies, but is wrong in other societies. It is wrong because it is prohibited by statute. Generally, *mala in se* crimes involve moral turpitude, while *mala prohibita* crimes do not." Id.
[78] See *Criminal Law*, R. Blanpain (ed), Kluwer Law International, Netherlands (2008), at 61.
[79] Joel Samaha, Criminal Law, Wadsworth, Cengage Learning, Tenth Edition, USA, 2011, at 11. *See also* Thomas J. Gardner and Terry M. Anderson, *Criminal Law*, Wadsworth, Cengage Learning, Eleventh Edition, USA, 2012, at 13. *See also* Glory Nirmala K. et al (2009), *Criminal Law I: Teaching Material*, Sponsored by Ethiopian Justice and Legal System Research Institute, unpublished, p.49.

invaluable manner. For the one who is the victim of, for instance, child pornography, racism, nazism, hate speech, or religious offence, it can be more than the property crime that she or he lost the cost of honor and morality. Moreover, computer crime can also highly affect individuals more than the property they might be loss. Assume, for instance, a computer criminal that alters medical prescription by hacking a certain hospital computer or alter the telemedicine, which causes the grave injury or death of the patient. Let alone the possible attack on life, there are also other personality rights which can be affected by computer crime i.e. right to privacy. Accessing a certain private data or computer system or network endangers the privacy right of individual. So it is hardly possible to measure costs of privacy in terms of property.

The Ethiopian ICT Policy and Criminal Justice Policy, though they have been adopted after the coming into force of the new Criminal Code, have given the due attention to the prevalence of computer crime. On top of that, the policies manifested the possible impacts of computer crime on the state, institutions, community and individuals. Thus, one can strongly argue that the legislature has failed to address the possible consequence of computer crime on state interest, institutional interest, community interest, and individual interest like life, health, privacy.

Generally, computer crimes should be schematized by the type of harm, the geographical location, the target or victim, and the perpetrator.[80] The harm caused by computer crime may consist of financial loss, invasion of privacy, information theft, destruction of trade secrets, meltdown of computer hard drives, or threats of public health or security.[81]

2.2.3. Punishment of Computer Crime under the Ethiopian Criminal Code:

Before rushing to the specific available punishments provided for computer crimes under the Criminal Code, it is necessary to conduct a cursor view of philosophical justification for imposing punishments and its proportionality. And then the specific computer crime punishment analysis has been conducted.

2.2.3.1. Justification of Punishment and Proportionality: General:

Punishment, which is a central concept in criminal justice system and entails loss of liberty, is one distinguishing feature of criminal norms. For the state to deprive citizen's liberty through the instrumentality of criminal punishment, therefore, requires strong justifications. Basically, there are two major theories for the justification of punishment i.e. the reductionist (as usually called as consequentialist or utilitarianism); and retributivists approach.[82] The consequentialist approach justifies punishment as an instrument of social control designed to reduce anti-social activity, mainly through deterrence, incapacitation, or rehabilitation; and tries to justify its future consequences (justified by consequences).[83] The retributivist approach justified punishment as an ill-deserted of the one punished or as a morally appropriate response to wrongdoing.[84] In other words, retribitivists justifies a particular instance of punishment by specific instance of punishment (justified by just desert).[85] As it is stated in different literature, there is other approach on the justification of punishment in between these two: mixed approach, which justifies a particular instance of punishment by both their consequence and the desert of the offender.

The justified punishments, to be effective, rather require additional principle of criminal law. One of the principles of criminal law which is highly relevant to this research is the principle of proportionality. The principle of proportionality, which is an imperative requirement for fairness, claims that "penalties be proportionate in their severity to the gravity of the defendant's criminal conduct."[86] The concept of proportionality suggests that punishment is appropriate where it is similar in magnitude to the crime.[87] The main concept of proportionality does not demand that the punishment be identical

[80] Michael L.Russtad, *Private Enforcement of Cybercrime on the Electronic Frontier*, Southern California Interdisciplinary Law Journal, Vol.11:63, 2001, at 65.
[81] *Id.*
[82] William Wilson, *Central Issues in Criminal Theory*, Hart Publishing, OXFORD-PORTLAND PREGON, U.S.A., 2002, at 43; *See also* Kevin M. Carlsmith, John M. Darley and Paul H. Robinson, *Why Do We Punish? Deterrence and Just Deserts as Motives for Punishment*, Journal of Personality and Social Psychology Copyright 2002 by the American Psychological Association, Inc. 2002, Vol. 83, No. 2, at 284–299.
[83] *Id. See also* LLOYD L. WEINREB, *Desert, Punishment, and Criminal Responsibility*, 47 Law & Contemp. Probs. 49 1986, at 47-53.
[84] Wilson, *supra* note 84.
[85] *Id.* at 54-61.
[86] Andrew von Hirsch, *Proportionality in the Philosophy of Punishment*, University of Chicago Press, Crime and Justice, Vol. 16 (1992), at 55.
[87] Thomas A. Balmer, *Some Thoughts on Proportionality*, OREGON LAW REVIEW, Vol.87, 783, 2008, at 784.

to the crime. Rather, the punishment ought to reflect the degree of moral culpability associated with the offence for which it is imposed. Certainly, the required elements for a certain crime are relevant in determining whether punishment is appropriately proportional.[88] Thus, the principle of proportionality is a balancing power of punishments that are too severe and too lenient. Accordingly, a given legislature that seeks to criminalize a given wrongful act is required to adopt punishments that are proportional to the specified offence. In other words, the legislature should establish penalties proportional to a particular offence by ranking offences and corresponding punishments.

2.2.3.2. Punishment of Computer Crime under the Code:

The Ethiopian Criminal Code, while the Code is drafted, as it is stated in the preamble, different discussions have been conducted with relevant bodies and the selected representative of the people. There is also a significant contribution of experts in different discipline and professional association. However, the increment of punishments regarding rape and aggravated theft is mainly on the basis of public opinion. In this regard, the role of experts and professional associations were insignificant.

The Criminal Code justifies punishments to deter the wrongdoer and potential wrongdoer (having the idea of deterrence). Imprisonment and death is justified to prevent the wrongdoers temporarily and permanently from committing further crimes (having the idea of incapacitation). Moreover, release of criminals on parole and probation has been allocated in the Criminal Code with a view to help wrongdoers to lead a peaceful life and considered it as rehabilitation. Furthermore, reformation of criminals in prison through taking part in vocational training and academic education in order to benefit them upon their release is the great concerns envisaged by the Criminal Code.

Under the Criminal Code, crimes are punishable in different levels. "Crimes of very grave nature" are punishable with "rigorous imprisonment" for the period of one year to twenty five or life[89]; and a "crime of not very serious nature" may subject to "simple imprisonment" from the term of ten days to three years.[90] "Petty offences" on the other hand, are punishable with fine or arrest for relatively shorter period of one day to three months.[91] To be more specific, the Code provides the punishments for computer crimes. Under the Code, for the offender who violets the computer crime provisions, are punishable from simple imprisonment of three months up to five years of rigorous imprisonment.[92] These are the minimum and maximum available punishment for the perpetrator that might loss liberty. Concerning fines, the floor and the ceiling of fines, according to the severity of the crime, ranges from two thousand birr to twenty thousand birr respectively.[93]

Computer crimes, which violets the privacy or the confidentiality of computer data of individuals, classified information of governments (against state security), and attacks the public morality, are punishable with the maximum of five years. Do these punishments are proportional to the gravity of computer crime? Will it have the required deterrence effect for those actual and potential wrongdoers? This is what the researcher wants to insight to the legislature or other respected body of the government. Assume, for example, a computer criminal, who accessed the government military or intelligence computer data or computer system or network and revealed to the world or the respected country and a country faced political crises and poor diplomatic relations with sister countries. And secondly, assume that the computer criminal accessed the network certain financial institution and through either altering or adding or deleting, transferred millions or billions of money to his account or someone else so that causes huge loss of money. Again, we can assume that alteration of certain medical prescription stored in hospitals computer can result death of many patients in the hospital or disseminating information through computer systems or networks which can damage the morals of the community is invaluable. So the available legal remedies for such types of grave nature computer crimes under the Criminal Code is maximum of five years imprisonment and twenty thousand birr as fine. Let alone the legislature or those experts and professional associations who were participated while the Code is dratted, a lay person can identify the disproportionate punishments proclaimed by such Code. From the very beginning while the legislature tried to justify for the new Criminal Code, computer crime seems the one that would be addressed properly. However, the gravity of the computer crimes and

[88] *Id*, at 86.
[89] See the Criminal Code, *supra* note 13, Art. 108.
[90] *Id*, Art. 106.
[91] *Id*, Art. 747.
[92] *Id*, Art. 706-709.
[93] *Id*.

the available legal remedies under the Criminal Code is incomparable. In other words, the punishment provided in the Criminal Code manifests the lenient attention given to computer crime by the legislature.

3. CONCLUSION

Computer crime or cybercrime is a term used to broadly describe a criminal activity in which a computer data or computer system or a computer network is a tool, or a target, or a place of criminal activity. Computer crime is not a distinct type of crime like traditional crime such as rape or murder and not limited to a certain jurisdiction. In other words, computer criminality is not limited to any specific type or any particular region or any particular target group. Computer crime is highly complex, self-reinforcing, technologically advanced, geographically widespread and indiscriminate. Computer criminals are varied in terms of age, skill and motives. So the targets of computer criminals can be data, networks or access that harm individuals, institutions, governments and countries which have no or weak criminal law with respect to computer crimes. Computer crimes or cybercrimes have a considerable impact on the national security of a given state, on the economy, on the privacy, on public morals and on life.

There are various international, regional and national initiatives and movements to combat computer crimes. At the national level, Ethiopian has set a legal framework specifically designed to combat computer crimes under various policies and a new criminal code.

The 2004 Federal Democratic Republic of Ethiopian Criminal Code has been enacted to address crimes such as computer crimes, which have emerged after the coming into force of the 1957 Penal Code. Thus, computer crime is not only an act prohibited by the law but also the core justification for the legislature to come up with the new Criminal Code. The Criminal Code prohibits unauthorized accessing, adding, altering, deleting or destroying a computer data, system, or network; and committing such acts with a view to steal, defraud, deceive, or extort or wrongfully control to obtain and importing, producing, selling, offering for sale, distributing, buying, or receiving or possessing instruments, secret codes, or passwords to further the commission of the specified computer crimes is amounts as a computer crime. However, the provided provisions under the Criminal Code are not sufficient to address the prevalence of computer crimes. Thus, computer crime do no treated as its nature, impact, and necessitated to adopt such Criminal Code. Let alone its insufficiencies, computer crime is characterized under the scheme of property crime. The harm caused by computer crime may consist of financial loss, invasion of privacy, information theft, or public health or security. Moreover, the legislature has failed to address the possible consequence of computer crime on state interest, institutional interest, community interest, and individual interest like life, health, and privacy. For those criminal cats, the available punishments under the Code ranges from simple imprisonment of three months up to five years of rigorous imprisonment and fine ranges from two thousand to twenty thousand birr. Thus, the provided punishment is disproportionate and manifests the lenient attention given to computer crime by the legislation.

The assessment of the Ethiopian legal framework to address the prevalence of computer crime is better in policy level than the Criminal Code. The 2009 Ethiopian National Information and Communication Technology Policy and the 2011 the Ethiopian Criminal Justice Administration Policy have given better attention to address computer crimes. The full implementation of these new policies requires many changes and additions to the existing laws, in particular the Criminal Code.

REFERENCES

[1] Decker, Charlotte, Cyber Crime: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, South California L.R. Vol. 81:959, (2008).

[2] Cyber Crime a Growing Challenge for Governments, KPMG International, Swiss, (2011).

[3] Grercke, Marco, Understanding Cyber Crime: Phenomena, Challenges and Legal Responses, ITU Publication, (2012).

[4] Aslan,Yasin, Global Nature of Computer Crimes and the Convention on Cybercrime, Ankara L.R, Vol.III No.2, (2006).

[5] Kierkegaard, Sylvia Mercado, Cracking down on Cybercrime Global Response: the Cybercrime Convention, Communication of the IIMA, Vol.V. Issue No.1, (2005).

[6] Franklin, Carl J., The Investigator's Guide to Computer Crime, CHARLES C. THOMAS-PUBLISHER, LTD. Illinois, U.S.A.,(2006).

[7] Kadir, Rizgar Mohammed, The Scope and the Nature of Computer Crime Statutes: A Comparative Study, German L.J., Vol. 11 No.06, (2010).
[8] Keyser, Mike, The Council of Europe Convention on Cybercrime, J. Transitional Law and Policy, Vol. 12:2, (2003).
[9] Ani, Laura, Cybercrimes and National Security: The Role of the Penal and Procedural Law, Law and Security in Nigeria, (2011).
[10] Council of European Convention on Cybercrime, ETS 185, 23.XI, Budapest, (2001).
[11] Criminal Code of the Federal Democratic Republic of Ethiopia, Negarit Gazzeta, Proclamation No.414/2004, 9th of May, (2005).
[12] Muthukumaran, B., Cybercrimes Scenario in India, Criminal Investigation Department Review, (2008).
[13] Chowbe, Vijaykumar S., The Concept of Cybercrime: Nature and Scope, Global Journal of Enterprise Information System, Vol. 3, Issue-1, (2011).
[14] Vogel, Joachim, Towards a Global Convention against Cybercrime, First World Conference on Penal law in Guadalajara, Mexico, (2007).
[15] Cybercrime Strategy, The Secretary of the State Presentation to the Parliament, Crown Publication, U.K., (2010).
[16] Singh, Pramond kr., Laws on Cybercrimes, Book Enclave, India, (2007).
[17] Marc D. Goodman, Why the Police Don't Care about Computer Crime, Harvard Journal of Law and Technology, Vol.10, No.3, (1997).
[18] Sieber, Ulrich, Legal Aspects of Computer-Related Crime In the Information Society, COMCRIME-Study, Prepared for the European Commission, Version 1.0, (1998).
[19] Elias N. Stebek, Principles of Ethiopian Criminal Law, St. Marry University College and USAID, Addis Ababa, (2013).
[20] Handerhan, Ryan, Japan and American Computer Crime Policy, Dietrich College Honors Thesis, Paper 69, (2010).
[21] Dashora, Kamini, Cyber Crime in the Society: Problems and Preventions, Journal of Alternative Perspectives in the Social Sciences, Vol.3, No.1, (2011).
[22] Ethiopia National Information and Communication Technology Policy and Strategy, (2009).
[23] Federal Democratic Republic of Ethiopian Criminal Justice Administration Policy, Ministry of Justice, (2011).
[24] Preliminary Analysis of the Legislation Requirements of the Criminal Justice of the Criminal Justice Administration Policy, Federal Democratic Republic of Ethiopia, (2009).
[25] O'Brien, Martin and Yar, Majid, Criminology: The Key Concepts, Routledge Press, London, (2008).
[26] Murado Abdo, Subsidiary Classification of Goods under Ethiopian Property Law: A Commentary, MIZAN LAW REVIEW, Vol.2 No.1, (2008).
[27] An Introduction to the Criminal Law of Afghanistan, ALEP, (2009).
[28] Pollock, Joycelyn M., Criminal Law, Matthew Bender & Company, Inc, 9th ed.(2009).
[29] Blanpain, R. (ed), Criminal Law, Kluwer Law International, Netherlands, (2008).
[30] Samaha, Joel, Criminal Law, Wadsworth, Cengage Learning, Tenth Edition, USA, (2011).
[31] Gardner, Thomas J. and Anderson, Terry M., Criminal Law, Wadsworth, Cengage Learning, Eleventh Edition, USA, (2012).
[32] Russtad, Michael L., Private Enforcement of Cybercrime on the Electronic Frontier, Southern California Interdisciplinary Law Journal, Vol.11:63, (2001).
[33] Wilson, William, Central Issues in Criminal Theory, Hart Publishing, OXFORD-PORTLAND PREGON, U.S.A., (2002).
[34] Carlsmith, Kevin M., Darley, John M. and Robinson, Paul H., Why Do We Punish? Deterrence and Just Deserts as Motives for Punishment, Journal of Personality and Social Psychology Copyright 2002 by the American Psychological Association, Inc. (2002).
[35] WEINREB, LLOYD L., Desert, Punishment, and Criminal Responsibility, 47 Law & Contemp. Probs. 49 (1986).
[36] Hirsch, Andrew von, Proportionality in the Philosophy of Punishment, University of Chicago Press, Crime and Justice, Vol. 16 (1992).
[37] Balmer, Thomas A., Some Thoughts on Proportionality, OREGON LAW REVIEW, Vol.87, 783, (2008).