ADDIS ABABA UNIVERSITY

COLLEGE OF LAW AND GOVERNANCE STUDIES

SCHOOL OF LAW GRADUATE PROGRAM

Master of Law (LL.M) in Public International Law

TELECOM FRAUD LAW AND THE PRACTICE IN ETHIOPIA:

CHALLENGES AND THE WAY FORWARD

A THESIS SUBMITTED IN PARTIAL FULFILLMENT FOR LL.M DEGREE

BY: HANA TESHOME

ADVISOR: MANDEFRO ESHETE (PhD)

March 2021

ADDIS ABABA, ETHIOPIA

DECLARATION

I, Hana Teshome, hereby declare that this thesis is my own original work. It has not been submitted for any degree or examination in any other university or program. All the materials I have referred in this thesis are duly acknowledged.

Declared by	**Approved by**
Hana Teshome	**Mandefro Eshete (PhD)**
Signature ----------	**Signature** ----------
Date ----------	**Date** ----------

ADDIS ABABA UNIVERSITY

College of Law and Governance Studies

School of Law

Graduates Programs Board of Examiners

Thesis Appraisal

Hana Teshome Gelalcha's thesis, entitled as **"Telecom Fraud Law and the Practice in Ethiopia: Challenges and the Way Forward"** is approved by the undersigned members to the examining board.

Board of Examiners	Signature	Date
Advisor: ----------	----------	----------
Examiner: ----------	----------	----------
Examiner: ----------	----------	----------

Table of Contents

ACKNOWLEDGEMENT

First and foremost, my gratitude goes to the almighty, thank you God for every blessing in my Life.

My heartfelt gratitude also goes to my thesis Advisor, Mandefro Eshete (Ph.D), for his guidance, support, swift comments and trust throughout my thesis work and beyond.

My colleagues, I'm very thankful for all your support particularly Million, for providing me your insightful ideas, expertise and smoothing things in the office.

Mr. Worke, Mr. Gemechu, Ms. Mignot, Chief sergeant Tadele all other volunteers who helped me formally and informally, I owe you.

My dear husband, very supportive, caring and my lifetime advisor, if the achievement in my studies is meant to be my success the credit is all yours. None of these would have happened if I did not have you by my side.

My sweet tastes of life Abrak and Melhiq, I have been taking away your precious time to accomplish this work. You two will have all my love and care from now on.

Families and friends who have supported and encouraged me in every way along this study, I'm very much indebted to you all.

To YETEMWORK

Dear mom, all of my success is dedicated to you, your bravery and altruism!

ABBREVIATIONS

CDRs	CALL DETAIL RECORDS
ECA	ETHIOPIAN COMMUNICATIONS AUTHORITY
EICTDA	ETHIOPIAN ICT DEVELOPMENT AGENCY
ETA	ETHIOPIAN TELECOMMUNICATION AGENCY
ETC	ETHIOPIAN TELECOMMUNICATION CORPORATION
FAGP	FEDERAL ATTORNEY GENERAL PROSECUTOR
GTP	GROWTH and TRANSFORMATION PLAN
ICFDS	INTERNATIONAL CALL FRAUD DETECTION SYSTEM
INSA	INFORMATION NETWORK SECURITY AGENCY
ICT	INFORMATION COMMUNICATIONS TECHNOLOGY
IT	INFORMATION TECHNOLOGY
ITIDA	INFORMATION TECHNOLOGY INDUSTRY
ITU	INTERNATIONAL TELECOMMUNICATION UNION
MINT	MINISTRY OF INNOVATION AND TECHNOLOGY
NISS	NATIONAL INTELEGIENCE AND SECURITY SERVICE
NTRA	NATIONAL TELECOMMUNICATION REGULATORY AUTHORITY
PTD	POSTS AND TELECOMMUNICATION DEPARTMENT
SIM CARD	SUBSCRIBERS IDENTIFICATION MODULES CARD
VoIP	VOICE OVER INTERNET PROTOCOL

ABSTRACT

Telecom fraud is generally defined as an abuse of telecom services, subscription frauds, bypass frauds and also dissemination of any illegal content via the telecom network. There are different types of telecom frauds and techniques; among others are sim box frauds, bypass fraud, and call termination.

The aim of writing this thesis is to assess the implementation gap, analyze practical challenges on the implementation of the telecom fraud proclamation which is enacted in 2012 and the discrepancies of some provisions of the proclamation with related laws specifically the computer crime proclamation. Based on the data collected from the key informants in this thesis, the executive organs specifically are facing several challenges while trying to implement the law due to failure of stating some crimes, improper determination of penalties, and failure of discharging responsibilities of organs and so on.

The thesis also examines the preparedness of the law ahead of expected shift in the telecom industry, i.e. liberalizing the market to private and international operators which might be a source of additional challenges to law enforcement on the telecom sector. This thesis recommends amendments for better implementation of the law and attempts to provide insights on how to improve the existing law in order to address encounters associated with upcoming shifts.

Key words: telecom fraud, bypass fraud, telecom fraud proclamation, computer crime proclamation, discrepancies, privatization.

CHAPTER ONE

INTRODUCTION AND OVERVIEW OF THE STUDY

1.1. BACKGROUND OF THE STUDY

In the world we live in today, telecommunication has become an integral part of our day to day life. The progress in to more and more of remote communication through telecom services have eased the way we do things and brought people around the world closer. In the meantime, public institutions, companies and individuals are continuously deploying data, sometimes confidential, in the cloud and are increasingly utilizing the service to complete tasks. Nonetheless, the ease and convenience of Telecom services has not come without challenges ranging from threats of mere crime acts to complicated cyber-attacks both on the data and infrastructure in the Telecom sector.

Historically, it is believed that telecommunication fraud become prominent after it first spread from Taiwan in the early 2000s which it was also known as "*Taiwan Fraud"* as it caused serious harm and social panic to the community.[1] Due to the fact that the Taiwanese have prior experience of telecommunication network fraud, they often seen as they themselves design the fraud acts[2] on telecommunications fraud which the mainland people follow that trend to make a fraudulent act.[3]

The criminals make the way they make telecommunication offences hidden and more "realistic' following the technological advancement of telecommunications network technology which also results at the infringement of personal information.[4] Consequently, the Taiwanese officials found different kinds of frauds in different districts which are deemed as the areas of source of crime of fraud. Some are like passing of acquaintances and leaders, changing flights, passing of online

[1] Huang Zuhe Causes and Prevention of Telecommunication Network Fraud, Post- Doctoral Research Center of CCISR, Haidian District, Beijing China, (ICHSSD, 2017), p.164.

[2] It was believed as they prepare a crime as a film script and others just take the script to commit telecom frauds.

[3] Huang Zuhe, (n 1).

[4] Id, p.165.

shopping, passing of public security, entertainment winning fraud and other many social service frauds and security frauds.[5]

As to the telecommunications fraud control association (2007), the Global annual economic loss of the world reached about 550-600 billion USD.[6] There are different causes of telecom fraud. Social distortion in the social transformation, violation of personal information, lack of responsibility of telecom and banks, low awareness of prevention of the crime, inefficient publicity of relevant authorities and severity of punishments to the people are among the main causes of telecom fraud crime.[7]

The increase of telecommunications network fraud crime with alarming rate, is followed by more and more hidden implementation of fraud. Some criminals commit "precision fraud" crime which is to mean that attacking targets successfully again and again and leading to more harm to the victims. Some main reason for this are, social values distorted in the period of social transmission, serious violation of personal information, the low responsibility of Telecom and banks, weak prevention awareness of the people, inefficient publicity of relevant departments, and severe punishment to the people.[8] These issues factor in to the criminals unstoppable effort of the commission of telecommunication service in a very sophisticated way.

Ethiopia, is not an exception for this challenging problem. Up until the enactment of the law to date, the executive organ face many challenges in implementing the law as it has some undefined but necessary terms and vague stipulations as well as discrepancies with other law. It could be even more serious considering the expedited privatization process that is going on in our country looking at the complex nature of the crime, the technological and infrastructural preparedness of the country.

The expected desire of the private companies which may force Ethiopia to liberalize some of the restrictions on the telecom services (for example VoIP which they inevitably want to provide to their customers) is also one of the reasons. Following this interest, there should be adequate legal

[5] Ibid.

[6]Ibid.

[7] Ibid.

[8] Id, p.167-169.

frameworks to administer related issues which in fact need a serious consideration. This in return widens the chance for more telecom fraud issues and obscures the litigation process if not addressed with up to date and clear legislations.

Despite ongoing efforts to govern the telecommunication services, the exponential growth in technology, users of the service and unmet demands still pose a threat to the Telecom operation. This calls for an adequate legal framework to administer related issues which in fact need a serious consideration.

More evidently, it is important to assess the status of telecom fraud offences and the existing legal framework in Ethiopia as it is an important component of public international law due to its transboundary nature and its potential effect on the public security.

1.2. STATEMENT OF THE PROBLEM

Even though the government of Ethiopia has put some measures in place to prevent and protect cyber-attacks including Telecom Fraud Offences Proclamation as one of the main moves, several violations have been made against the law since its enactment. The legal gaps that are not addressed properly in the Telecom Fraud Proclamation coupled with the lack of judiciary awareness on arbitrary provisions also leaves individuals susceptible for trials filled with subjective interpretation and litigators' twist. Some of the problem emanates from improper definition, failure to provide definitions to some terms, misinterpretation and some overlapping provisions with the Computer Crime Proclamation no.958/2016.

The first problem essentially stems from the term telecom fraud, which has not been defined in the telecom fraud proclamation despite the fact that it is the core concept and is crucial to have a clear understanding of the term while we are tending to regulate offences related with telecom products and/or services. Therefore, definition remains to be a fundamental ambiguity that leads to crimes committed using such loopholes that the law left unregulated.

Through scrutiny of some provisions of the telecom fraud offences and computer crime proclamations, it was also evident that there are different definitions provided for similar acts, double criminalization and different level of penalties laid for similar offences which tops up on the challenges posed by the lack of clear definition.

A specific example includes; the Telecom Fraud Offences Proclamation states in its definition Art 2(3) a "Call back service" as it is an act of bypassing and it is punishable with 5yrs-10 years of imprisonment. But this definition cannot be referred as a call back service; it's rather a call termination act. Instead it's the bypass fraud that needs to be defined in this manner since the entire part of the law mostly referred the act of bypass fraud. There is also a penalty laid for the act of bypass fraud with 10-20 years of imprisonment which overlaps with the above penalty rate which also amounts as double criminalization.[9]

Based on an interview conducted[10] the Telecom Fraud Offences Proclamation doesn't specify anything about the registration and distribution of sim cards which the police always suffer to handle cases committed with sim cards. The police caught so many sim cards even with a single individual while conducting an operation but left with no law to accuse those individuals only for caught with those amounts of sim cards since the law doesn't put minimum or maximum number of sim cards that a person can have at a time nor require a registration.[11]

The law gives a mandate to the Ministry of Innovation and Technology (this power is now of course, transferred to the new Ethiopian Communications Authority) to provide list of type approvals and standards for the importation, manufacturing and assembly of telecom equipment as its stated under Article 3. But nothing has happened so far. The police and prosecutors face a challenge while investigating a case, since they are obliged to wait for the approval every time for a certain equipment to determine whether its allowed for individuals or not.

Therefore, it is evident that there are plenty of reasons to examine the theoretical and practical gaps of Telecom Fraud Offences Proclamation. The upcoming developments and effort to the telecom privatization also demands a closer scrutiny of the existing law. Thus, this thesis

[9] Telecom Fraud Offences Proclamation, 2012, Proclamation No. 761/2012, Fed. Neg. Gaz, year 18. No. 61, Article 8 (1) (2).

[10] Interview with Chief Sergeant Tadele Wubetu, Federal Police Crime Investigation, Financial and Property based Crimes Investigation Unit, Crimes against Governmental Institutions Secretariat Office, Supervisor, held on 26 October 2020, 2:30 PM.

[11] Ibid.

endeavored to examine the existing telecom fraud offences proclamation with regard to its sufficiency, the implementation gaps Vis a Vis practical challenges and the lacunae thereof.

Therefore, indeed is the Telecom Fraud Offences Law comprehensive enough to regulate existing and upcoming practical legal challenges?

1.3. RESEARCH OBJECTIVE

1.3.1. GENERAL OBJECTIVE

The general objective of the study is to assess whether the existing Telecom Fraud Offences Proclamation is sufficient enough to govern every legal and practical aspects as well as new challenges ahead.

1.3.2. SPECIFIC OBJECTIVES

The specific objectives are to:

- Examine the status of Telecom Fraud Offences Proclamation entirely with the implementation gaps and challenges.
- Identify the contradiction of the Telecom Fraud Offences Proclamation with other law/s and practical cases.
- Identify gaps that hinder the current law from administer the new agenda efficiently i.e., privatization of the telecom sector.
- Analyze and pinpoint prospects for the next step towards the law.

1.4. RESEARCH QUESTIONS

1.4.1. CENTRAL QUESTION

1.4.1.1. Does Ethiopia have a comprehensive legal framework to govern telecom fraud offences and practical challenges properly?

1.4.2. SPECIFIC QUESTIONS

1.4.2.1. Does the current Telecom Fraud Offences Proclamation address/ govern telecom fraud offences properly?

1.4.2.2. Are there any contradictions between provisions of laws addressing similar/related offences?

1.4.2.3. What are the drawbacks that existing laws might have in the event of having multiple and international telecom service providers in Ethiopia?

1.4.2.4. How does the entry of multiple telecom service providers affect the execution and/or the revision of existing proclamation?

1.5. RESEARCH METHODOLOGY

The research is conducted using a qualitative approach while examining data and information in order to have comprehensive assessment to answer the research questions. This approach involves gathering firsthand information from key informants on the subject particularly to address a research problem in which lack substantial reference material.[12]

This research is also doctrinal through which both primary and secondary sources are consulted. In the consultation of primary source, domestic laws, an archival study of the Telecom Fraud Offences Proclamation are evaluated in order to have extensive understanding.

The secondary sources include books, relevant literatures, articles and credible internet sources. The methods also included as evaluating materials that are relevant to this work which are found in both hard and soft copies. A comparative analysis has been made as to some legal experiences of telecom practices of some countries which they are worth considering in different perspectives.

Four countries are consulted in this regard are: Egypt, Myanmar, Kenya and Ghana based on their relatively economic status, demographic, political unrest, and level of technological advancement and prior experience on telecom privatization.

An interview has also been conducted with one expert from Information Network Security Agency (INSA) who is an expert on the subject area. Another interview had also been conducted with an officer from Ethio-telecom for his legal experience in the company, a FGAP for her exposure to court cases on related matters, and a police officer from the federal police crime investigation unit hoping to get honest and significant inputs for this thesis. The number of

[12] John W. Creswell, Research Design, Qualitative, Quantitative and Mixed Approaches, (4th ed. 2014), p. 16.

interviewees from each organization has been decided as to their expert knowledge and practical experiences to the intended law and practice. All of them are told about the general idea of the research and specific questions which all of them were volunteer and keen to collaborate.

1.6. LITERATURE REVIEW

Various countries have developed prevention and mitigation strategies that have progressively attempted to monitor, detect, isolate, prevent and address threats on both the data and telecom infrastructure. However, alleged cyber security attacks and related activities have surfaced countless times. Governments around the world, including Ethiopia have passed various laws in order to mitigate such offences. The Telecom Fraud Offences Proclamation No.761/2012 enacted to prevent and control offences related with telecom fraud is one of them in Ethiopia. The Computer Crimes Proclamation No.918/2016 which in other words proclaimed to prevent and control offences related to computer and computer systems also has some overlapping provisions with that of the telecom fraud offences law.

Historically, the Ethiopian Telecommunications Agency (ETA) was established by the Telecommunications Proclamation No. 49/1996, (as amended in 2002) having a responsibility of regulating the telecom industry until the Ethiopian Government realizes the converging trend of telecommunication, broadcasting and ICT sectors in 2011.[13]

ETA continued its mandate across the regulatory divide sharing responsibilities with the Ethiopian ICT Development Agency (EICTDA) which is also initially established to regulate and support information technology (IT) services in the country. Consequently, the then Ministry of Communication and Information Technology (MCIT) established by Proclamation No.691/2010 (as amended in 2011) following the effort made by the government toward sector reform. Thus, in this regard, MCIT has took power of every aspects related to communications which was handled by the former Ministry of Transport and Communication as well as the regulatory powers of ETA and EICTDA.[14] Consequently, a new directorate has been established

[13] Kinfe Michael Yilma and Halefom H. Abraha, The Internet and Regulatory Responses in Ethiopia, Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media, Oct. 2015, p.115.

[14] Ibid.

under MCIT in order to undertake regulatory issues of telecommunications, postal and technology.[15]

The Telecommunication reform in Ethiopia began in 1996 with the enactment of a law that created a single operator since the then Ethiopian Telecommunications Authority has been served as both Telecommunication Service provider and regulator. The 1996 law then abolished Ethiopian Telecommunication Authority by separating provision from regulation with the establishment of two entities, i.e. the ETA and the Ethiopian Telecommunications Corporation (ETC) as a regulator and government owned monopoly sole provider respectively.[16]

It is after the Ministry of Communications and Information Technology established in 2010 that new departments of the communications and IT standardization and Regulation Directorate which handle all regulatory issues entirely.[17] The monopoly of the government hinders the sector to register significant development despite the Governments ambitious investment in the infrastructure.[18]

In this regard studies had shown that pro-competition policy intervention is important to deal with service penetration, low quality of service and high cost of broad band access.[19]

Absence of researches/articles made on this specific topic leads the researcher to make further investigations on the entire law and implementation gaps of telecom fraud law and practice.

The aim of this thesis is therefore assessing the existing legal framework on the telecom fraud offences and then having a close scrutiny on the legal gaps and practical challenges. This thesis also focuses the current status of the existing law in light with the dynamic nature of the crime and analyzing whether it has a sufficient room to regulate the upcoming event or not.

---

[15] Ibid.

[16] What Lessons Can We Learn, Review of the Legal and Regulatory Frameworks in the Information and Communications Technology Sector in a Subset of African Countries, United Nations Economic Commission for Africa, first printing July 2017, p.13.

[17] Ibid.

[18] Ibid.

[19] Lishan Adam (2010). Ethiopia ICT Sector Performance Review 2009/2010, Towards Evidence-based ICT Policy and Regulation. Volume 2, Policy Paper 9, 2010. Johannesburg: Research ICT Africa.

1.7. SCOPE

The scope of this thesis is limited to assessing the legal gaps and practical challenges of existing Telecom Fraud Offences law of Ethiopia. It is limited to examining issues associated with operational interpretation of the existing Telecom Fraud Offences law against crimes stipulated within the same legislation alone. It does not analyze the Computer Crime Proclamation but uses the legislation in reference with the Telecom Fraud Offences law to show conflict definitions and articles in lieu of portraying the legal gaps and associated practical challenges. Assessing the preparedness of the existing law in relation to upcoming liberalization of the telecom sector is also covered within this thesis.

1.8. SIGNIFICANCE

This research will inform legislators to consider changes towards the revealed gaps of the existing law. Knowing that there are some moves to amend the telecom fraud proclamation, this research will provide key ideas worth considering. It will also indicate how and what necessary measures would have to be taken moving forward as Ethiopia is planning to have a new policy on liberalization of the telecom industry.

1.9. LIMITATION

The current situation in the world and in Ethiopia hindered the researcher from moving freely here and there to collect relevant information as most people are not easily accessible due to the Covid 19 pandemic. The restrictions that most organizations took as a measure to contain the spread of Covid 19 has also another challenge for the researcher since internet access is limited at home which incapacitated the researcher from searching materials exhaustively. In addition, people are not willing to talk in person in fear getting in contact with Covid 19 infected person which also imposed limitation on free communication and hence, hampered the chances of getting further relevant inputs.

1.10. THESIS ORGANIZATION

This thesis is organized in four chapters. The first chapter of this thesis has introduction that encompasses background, statement of the problem, objectives, research questions, methodology, literature review, scope, significance of the study, and limitation of the study.

Chapter two discusses the conceptual framework of telecom fraud offences and made a comparative analysis of state experiences. Chapter three discusses the legal gaps, practical challenges on implementing the law and made a brief analysis on the findings which also gives some insights towards the approaching upcoming event. Chapter four consists of conclusion and recommendations.

1.11. THE PREFERRED RULE OF CITATION AND REFERRENCE

This thesis has referred the Addis Ababa university school of law LLM thesis guideline for its referencing style.

CHAPTER TWO

THEORETICAL FRAMEWORKS AND COMPARATIVE ANALYSIS

2.1. TELECOM FRAUD: CONCEPTUAL FRAMEWORK

Telecommunications fraud generally is that obtaining a telecom service without the intention to pay or the use of telecommunication service to commit other criminal acts provided by law using the telecom network. [20] Technically, it means that the transmission of voice or data across a telecommunications network with the intent to avoid or reduce legitimate call charges.[21]

It has been a serious threat to the sector since it is possible to be committed by a teenager level from the linear services up to the well-organized groups and organization to disrupt the whole telecom service.[22]

Telecommunications fraud (aka Telecom fraud) refers to the abuse of telecommunication products (telephones, cell phones, computers etc.) in which victims include consumers, businesses and communication service providers.[23]

2.1.1. CLASSIFICATIONS OF TELECOM FRAUD

There is a distinction between telecom fraud and methods of the execution of the fraud which the former is as we see above an intention of misusing telecom services and/products while the latter mean that a technique or way of interception for the illegal intent.[24]

Telecom fraud can be categorized into four groups, these are: -

Contractual fraud: frauds like subscription fraud and premium rate fraud which are intended to use a service but having no intention of paying are categorized here.

---

[20] Godfred Yaw Koi-Akrofi, Joyce Koi-Akrofi, Daniel Adjei Odai, and Eric Okyere Twum, Global Telecommunications Fraud Trend Analysis, Feb. 2019, p.941.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

Hacking fraud: a revenue is generated here by breaking into secure systems such as PABX[25] fraud and network attack.

Technical fraud: attacks against the weaknesses in the technology of the mobile system, needs some technical knowledge and ability then it can be distributed to the non-technical ones too. Cloning and some technical frauds are of specific examples.

Procedural fraud: against the procedure employed to minimize exposure to fraud and often attack the weakness in the business procedures used to grant access to the system. Roaming fraud, voucher ID duplication, and faulty vouchers are among procedural fraud.[26]

Fraud has a negative impact on every situation since it violates the trust between people or towards institutions for specific services and/ or products. Telecom fraud though is currently becoming more prevalent threat for the telecom industry.

There are different kinds of telecom frauds as well as several methods of committing the offence. Some of the types of the frauds committed against the telecom services and/or products include arbitrage, call and SMS spamming, domestic revenue share fraud, international revenue share fraud, phishing, premium rate service fraud, and roaming fraud.[27]
The methods of committing these frauds are such as;-

Subscription fraud: this type of fraud has come from an intention not to pay for the services and sought illegal means to escape from being charged. Mostly the fraudsters use their own, stolen or fabricated identity to do such acts.[28]

Private Branch Exchanges (PBX): these are telephone set ups targeted for hacking into enabling calls. It is utilized by little and medium organizations for internal and external communication.[29] PBX is also described as a private telephone network in the office which seems difficult to get private line for each employed individual. So, a PBX system enables calls

[25] It is a toll fraud also known as 'Phreaking' is when hackers fraudulently access the company's PABX system and uses it to make expensive long distance calls.

[26] Godfred, (n 20).

[27] Ibid.

[28] Id, p.943.

[29] Ibid.

between users on local line which also making them to make external call with many external phone lines outside of PBX.[30]

Bypass Fraud: the most prevalent method of telecom fraud in these days are bypass fraud and international revenue share fraud (IRSF). In bypass fraud sim boxing[31] connects incoming VoIP calls to local networks through SIM cards and cellular radios which transported at lower domestic rate and freed international call tariffs.[32]

2.1.2. FEATURES OF TELECOM FRAUD

Telecom fraud has its unique characteristics since it is always under change and mainly technologically oriented. Some of the features include;

2.1.2.1. Transboundary: it has been said that the telecom fraud is a transboundary crime because the actors and the target body may not be necessarily in same place. It can be from anywhere to cause a damage on a certain telecom service found anywhere in the world. For instance, significant number of a call termination crime committed in Ethiopia from sim box machines found in neighboring countries.[33] This makes the investigation and controlling of the crime very difficult.

2.1.2.2. International Collaboration: since the actors of telecom fraud can be individuals, telecom network operators, terrorist organizations, international telecom product manufacturers, this entity may cooperate to organize the fraud act in different locations. Again, in Call termination act, actors like the international network operator, brokers, and owners of sim box machines may collaborate jointly and will have a share from the income.

2.1.2.3. Complexity: though the telecom fraud is committed anonymously using different identity hiding technologies, not to be seen for the executive easily. The fraudsters may not be necessarily found at the place of the crime scene rather using remote technologies and can do it

[30] Ibid.

[31] It is the most common implementation of interconnect bypass.

[32] Godfred, (n 20), p.945.

[33]Information Network Security Agency, Report, November 2016.

by proxy as well. The convergence of the telecom industry with the internet technology also increases the complexity of the crime.

2.1.2.4. Cost Effective: comparing the gains after the execution of telecom fraud, the cost that the actor/s may incur during the process is minimal.

2.1.2.5. Dynamic Nature: as we know that the information technology era is unique by its fast-dynamic trait. The telecom fraud is also following this nature. The fraudsters update continuously their methods and ways of committing the crime using this feature of the technology.

2.1.3. CAUSES OF TELECOM FRAUD

There are different causes we can mention that caused the telecom fraud crime. Distorted social values due to social transformation, serious violation of personal information, the low responsibility of telecom and financial institutions, weak awareness of the public towards prevention, inefficient publicity of relevant departments are among them.[34]

2.1.4. PREVENTION MEASURES OF TELECOM FRAUD

There are different measures taken for different frauds as to the methods they are conducted. For international call fraud detection for instance, there is a proposed technique of classification the CDRs for roaming subscribers.[35] The ICFDS[36] will receive call detail records (CDRs) for international roamer that receive from clearing house.

Some suggested that a response to telecom fraud shall include; construction the moral of the citizen since people tend to use their money even to violate rules. Some business institutions are also part of this mischief that they don't get critical what they customers are do.[37] Increasing the Protection of personal information in addition to strengthening the publicity of personal information is also essential that the community by itself can take immediate actions to fight

[34] Huang Zuhe, (n 1).

[35] Arif Bramantoro, Yousef Alaraouji, International Call Fraud Detection Systems and Techniques, Conference Paper, Research Gate, September 2014.

[36] International call fraud detection system.

[37] Huang Zuhe, (n 1).

such offences.[38] Banks and telecom operators shall enhance their supervision to implement the 'real name' system for mobile phone by making responsible the telecom operators by law as it is strictly enforced by banks.[39] Raising public awareness of fraud prevention, giving an equal emphasis on Civil and Criminal Laws which may create attention in the community, enhancing the cooperation with the international community are considered as the pillars to combat the telecom fraud crime and its consequences.

In addition, there are also several key suggested components put to a fraud detection system. These are a continuing source of call detail data, a database to store the data, a set of detection algorithms, People to verify fraud and implement corrective measures, and Visualization tools to help people make diagnoses.[40]

2.2. COMPARATIVE ANALYSIS OF BEST EXPERIENCES ON LEGAL RESPONSE TO TELECOM FRAUDS

As the information technology market develops around the world, countries are finding a way to regulate the sector-oriented approach that lay prohibitions on certain activities of telecom services.

In countries where strong state intervention applied and information technology service providers owned or supported by the government, face challenges while trying to regulate where there was no legal precedent and experience.

The regulators these days are thinking about addressing issues of telecom frauds which were not an issue several years ago since they need to be attentive and responsive to cases arise from these new technologies and related services.[41]

The following countries are among some of the best practices in the governance of telecom fraud which are chosen based on their relatively similar situations in capacity, technological

[38] Ibid.

[39] Ibid.

[40] Richard A. Becker, Chris Volinsky, and Allan R. Wilks, Fraud Detection in Telecommunications: History and Lessons Learned, Article in Technometrics, February 2010, p 21.

[41] ICT Regulation Toolkit, Legal and Institutional Framework, ITU, infoDev, May 2016, p. 10.

advancement, political interest and some efforts made to liberalize the telecom market in their respective countries.

2.2.1. EGYPT

Egypt has been a member of ITU since 1876.[42] The telecommunication is governed under the regulation No. 10/2003 which is also known as the Telecoms law. The anti-cybercrime law is also enacted recently in 2019.

There are three major authorities regulate the fields of telecom and media in Egypt. The General Authority for investment and free zones, the National Telecommunication Regulatory Authority (the NTRA) established by the telecoms law and affiliated to the Ministry of Communications and Information Technology, which organizes the telecommunications sector, and the Information Technology Industry (the ITIDA) established by virtue of the E-signature Law.[43]

The NTRA regulates the communications sector in Egypt. The core mission of the NTRA is to encourage national and international investment within free competition rules as the Egyptian government endeavors toward the formulation of free-market and business-friendly policies. The establishment of regulatory body in EGYPT is in the legal form of an independent public authority.

The Law of Egypt prohibits *establishing or operation telecommunication networks, establishing telecommunication networks infrastructure, providing telecommunication services, bypassing international telephone calls by any means whatsoever*[44]*, annunciation, publishing or recording, hiding changing, obstructing or altering telecommunication messages, divulging without due right any information concerning telecommunication networks users or their incoming or outgoing communication,*[45] import, manufacture or assemble any telecommunication equipment without prior license from authority, universal service obligations and services.

The actors of the specified offences in the telecoms law shall be liable to simple or vigorous imprisonment to various amount of fine as per their degree of the offence. Not less than 3 months

[42] Al Kamel Law Office, Telecoms and Media, An Overview of Regulation in 48 Jurisdictions Worldwide, Egypt, 2011, p.133 ff.

[43] Ibid.

[44] Egypt Telecommunication Regulation Law, Law No. 10 of 2003, February 2003, Article 72.

[45] Ibid, Article 73.

to 5 years and 500,000 pounds and in some offences, there may be a multiplication of several times of the income gained from the illegal activity.

With regard to the share of public-private ownership, the state of Egypt owns the greater part of telecom Egypt's stocks, amounting to 51%. It means that the rest 49 percent is left for the private sector. Foreign ownership restrictions do not apply to authorization to provide telecom services in Egypt.

Egypt is cooperating with the private sector to improve telecom, liberalizing the telecoms market, and committing to the universal service policy while rapidly setting up modern telecommunications networks and services. Hence the National Telecoms Master plan was drafted by the government in cooperation with the private sector.[46]

Later, Egypt introduces the Anti-Cybercrime Law in 2018, Law No. 175/2018 on combating information Technology crimes as a whole.

The Anti-Cybercrime Law regulates activities online, and, according to official statements, it aims to complement the new press and media laws, which penalize, *inter alia*, unlicensed online activity and content violations, such as fake news. According to Article 44 of the new law, the Prime Minister will issue Executive Regulations within three months of the 15th August 2018 enactment date. Under Article 43, telecommunication service providers and other addressees of the law have a one-year transitional period during which they must bring their activities in line with the Anti-Cybercrime Law.[47]

It covers offences against confidentiality, the integrity and availability of computer data, computer related offences, content related and so on. The addressees are; natural and legal users, service providers, managers of legal persons, web administrators and state officials.

The penalties here include imprisonment of up to two years and fines of up to 10 million Egyptian pounds.

The investigating authority, judges, public prosecutor granted the power to investigate, giving an order of shutting down websites, etc. and in some cases the authorities may also access, seize, trace, or attach data for a specific period of time by the law for further investigation.[48] The power

---

[46] Al Kamel Law Office, (n 42).

[47] https://www.lexology.com/library/detail.aspx?g=90440972-f53e-46dd-b225-7f7cbdea7d73, last accessed, 10/11/2020, 1:36 AM.

[48] Ibid.

of the Egyptian authorities even extends up to claim a criminal jurisdiction upon non Egyptian citizens for crimes punishable under the Cybercrime law and also if criminalized under the national law of the country where the crime is committed. Actions are also taken outside Egypt against web pages or the bodies who operate them.[49]

2.2.2. MYANMAR

> *With one of the lowest wireless penetration rates in the world, Myanmar's telecommunications sector is positioned to witness robust growth in the coming decade.'*[50]

After spending half a century under military rule and engaging in civil wars, Myanmar remains one of the poorest countries in the world. The revival of the country reforming in many sectors also motivate the telecom industry which it poised for a boom after decades of poor connectivity. In order to curb the weak situation in the telecommunication sector, Myanmar decides to liberalize and enter private telecom operators into the market deeming that it will be the key to the successful development of telecommunication sector that without market liberalization the growth of the telecom industry become unimaginable.[51]

Consequently, two new licensees have been selected to provide telecommunications services in Myanmar as integrated license operators. The telecommunication law is also promulgated in 2013 which allows international and domestic private sector can participate in free and fair competition.

Going through this and many more reforms in the telecom sector, especially regulating it, Myanmar's regulatory bodies lay under the control of the Government by dividing tasks for different bodies of the country while it was under full monopoly of one party in the previous administration.[52] In this regard the Myanmar's Ministry of Transport and Communications' Posts

---

[49] Ibid.

[50] Deloitte, Southeast Asia Ltd, Myanmar, the next Asian telecommunications Greenfield? 2013, p 1-7.

[51] Ibid.

[52] Freedom House, *Freedom on the Net 2018 - Myanmar*, 1 November 2018, available at: https://www.refworld.org/docid/5be16b03a.html, accessed, 10/23/2020, 12:10 AM.

and Telecommunications department (PTD) took the mandate for regulating telecommunications in the country which previously served as a sole provider to all telecommunications services.[53]

2.2.3. KENYA

Our neighboring country Kenya has a regulatory framework on different technological issues in a single document. The Kenya Information and Communications Act consists of provisions on telecommunication services, radio communications, broadcasting services, postal services, licensing, electronic transactions, universal service fund and others are among them.[54]
Authorities: The Minister of communications and the communications commission are jointly responsible to regulate generally telecommunication services.[55]

The offences relating to telecom services in Kenya include, improper use of system, alteration of messages, interception and disclosure, tampering with telecommunication plant, severing with intent to steal, trespass and willful obstruction, and prohibition of unlicensed telecommunication system.[56]

In Kenya internet calls made into phone calls both locally and internationally are allowed, with the only prerequisite is that the service provider must be licensed by the authority.[57]

Making calls through fixed line phones using the internet network is also allowed in the Kenyan Law which again asks for the appropriate license that the Law also expected to legalize voice calls that are made from fixed lined to the internet platform.[58]

It is obvious that the telecommunication equipment and/ or services are integrated with computers and/ computer networks. Hence it seems that there is no need of making a distinction between the two while they are highly integrated.

---

[53] Ibid.

[54] Kenya information and communications act, Chapter 411A, Laws of Kenya, Revised Edition 2012 [1998], Published by the National Council for Law reporting with the Authority of the Attorney- General, www.kenyalaw.org.

[55] Ibid.

[56] Id, Arts.28- 34.

[57] Ibid.

[58] The law asserts that this service will also be allowed considering the future technological advancements.

Concerning the VoIP services, all types of VoIP s are allowed in the Kenyan Law.[59] Except the laws which are applicable while the VoIP are commercialized, the same Law applied for internet services are also applicable for VoIP. There are also no extra charges needed for VoIP other than the regular internet fees while using the internet service.

2.2.4. GHANA

MTN Ghana is one of the famous telecom operator as it is working in many other African countries,[60] is also leading in the highly competitive telecommunication industry zone in Ghana. As many other African countries Ghana is also challenged by telecom fraud crimes such as sim box fraud and interconnects bypass frauds. The authorities of Ghana took a measure that avoiding more than 300,000 sim cards which were used for sim box fraud.[61] They have used an application called Geo-location to identify locations where sim box frauds are committed to institute a case against the offenders.[62]

Sim box frauds in Ghana mostly are caused by failure to have a full profile of the customers, failure to block sim cards forthwith the sim box frauds, and the difference in local and international call tariffs.[63] If the tariff for both calls be the same there will not be sim box and interconnect bypass fraud but this could not be possible since the foreign currency from international tariff is very essential to the Economy of Ghana. So that Ghana tends to take other measures for the mitigation of this fraud.[64] Some of them are; active detection; it uses to trap sim box fraudsters at the time of the offence by coordinating with other foreign operators. Passive detection; this one is that detecting the calls after they conducted with the system knows it was from sim box machine or not.[65] The other system Ghana deploys is that identifying the

---

[59] Guidelines for the implementation and provision of VoIP Services, Communication Commission of Kenya, 2005.

[60] It's now reached to 22 African countries after established in Johannesburg, South Africa.

[61] Telecoms: Ghana Seizes 300,000 Sim Boxes from Syndicates, by Dasmani Larii, posted on Friday, 8 April 2016 10:54, Last Accessed 11/2/2020, 11:55PM.

[62] Ibid.

[63] Ibid.

[64] Ibid.

[65] https://africabusinesscommunities.com/news/mtn-remains-committed-to-fight-against-simbox-fraud.html, last accessed 11/2/2020, 3:56 AM.

location of sim boxes and blocks them immediately. There are also reporting mechanisms for the customers and telecom staffs at any time to give information if they found any suspect.

MTN Ghana is also a victim of sim box fraud which makes it loss a lot. It also took some technical measures even it allocates a lot of money in a month to control it.

The other measure taken by the Ghana operators is that asking the customers to bring standard identity cards while they came to buy or distribute sim cards and also investigating duplicate sim cards in the name of one customer/operator.[66] Preparing and publicizing the Legal and regulatory frameworks are also taken to control and punish the fraudsters. Specifically, Ghana took administrative measures on the telecom staffs since they are involved in most of the crimes.[67]

2.3. LESSONS LEARNT FROM EXPERIENCES

A comprehensive regulation of telecom services, implementation of telecom fraud offence laws and hosting private telecom companies are considered as a common denominator that we can draw a lesson. Egyptian government allows for the free market and formulates business friendly policies which our country with same free market policy need also to consider suck kind of strategies in liberalizing the telecom market. It's also good to be aware about the technological advancements of Egypt since we have an antagonist interest so that we can be take measures accordingly.

Myanmar has been in a long political unrest since it has become to the reform. The technological reform is thus among the most successful it has made so far. Besides the efforts made towards interconnectivity of the nation, the entrance of private telecom companies and better operations due to the conveniences made to them shows us how the country aggressively works best. This should be seen as a good indicator for us while our country is now suffering with internal turmoil since the 'reform' has taken place.

Kenya, we have a lot to take from our neighboring country in respect to telecom services and from its comprehensive legal frameworks. The Kenyan law has same regulation for both telecom and computer crimes deeming that both are of same nature. The other lesson here is that Kenyan

[66] Telecoms, (n 61).

[67] Ibid.

law does not prohibit VoIP which Ethiopia should consider this since it never protects the crimes prohibiting by law which we always observe VoIP's here and there. Who else is not using it anyway?

Ghana has a renowned private telecom operator involved in the market and work jointly with the government to prevent and protect the telecom fraud offences. This also can be taken as a good opportunity for us since we are a late comer to this event which the private companies need a certain safe zone while giving their services as well as we need to know how we can manage security issues thereof. It is also better to pick private companies with good reputation for instance MTN of Ghana is reached more than 22 countries in Africa by now.

CHAPTER THREE

TELECOM FRAUD LAW AND THE PRACTICE IN ETHIOPIA

In Ethiopia, internet coverage generally is still to be said at its infancy stage with small number of users relatively with some neighboring and sub-Saharan African countries.[68] Our country has been among the most expensive broadband in the world as the international telecommunication union (ITU)[69] has referred.[70] Even if it's much better now in subscription rate, the mobile rate and low connection of the internet is still a problem to the users.[71]

Ethio-Telecom is striving to achieve high level of telecom services as it has given prior attention from the government in the GTP 2[72]. Making telecom provider upgrades to meet international standards, the use of domestic products and services, and the establishment and effective enforcement of comprehensive policy and regulatory frameworks to prevent and control illegal activities in the industry are the three main strategies to implement the intended growth by the plan.[73]

Facebook is for instance the leading platform used by the youth while others are followed in many developing countries including ours.

---

[68] For instance, Kenya has high number of subscriptions with relatively better network coverage and quality since it hosted private and international operators which also extends to the financial sector like MPESA.

[69] International telecommunication union is a global agency for telecommunication issues, provide assistance by doing annual survey and report of global telecommunication status with recommendations.

[70] Article 19, Ethiopia: Proclamation on Telecom Fraud Offences, Aug. 2012, p.15. The ITU further link low penetration levels and relatively high prices for mobile telephone services are the consequences of a lack competition and a failure to liberalize the Telecommunication Sector.

[71] Ibid.

[72] Federal Democratic Republic of Ethiopia, Ministry of Finance and Economic Development, Growth Transformation Plan (GTP 2), 2010/11-2014/15, 2010, p 75.

[73] https://www.ethiotelecom.et/%e1%8b%a8%e1%8a%a2%e1%89%b5%e1%8b%ae-%e1%89%b4%e1%88%8c%e1%8a%ae%e1%88%9d-%e1%8b%a8%e1%88%a6%e1%88%b5%e1%89%b5-%e1%8b%93%e1%88%98%e1%89%b3%e1%89%b5-2013-2015-%e1%88%b5%e1%89%b5%e1%88%ab%e1%89%b4/

Ethiopia as a developing state has been doing many improvements on the development of telecommunications since it's considered as one of the strategic priorities in the 5 years GTP.[74] Since then Ethio telecom[75] (the then ETC) has been through a lot to improve the services as it aiming now in its three years strategy[76] addressing ever changing customer demand, digital inclusion to create better digital economy, enhance productivity, shift the revenue from traditional revenue streams to value added and content driven services by introducing new business streams and solutions like Internet of Things (IOT), Application Programming Interface (API), and other new services.[77]

Even if technological oriented and upgrading the services, telecom fraud still is a challenge for the emerging telecom industry in our country. In fact, the more telecom services are adopted in the country the more to get risks to be exposed for frauds.

There have been some governmental institutions to overtake the surveillance apparatus in the history of Ethiopian telecommunication. The Ethiopian telecommunication agency[78], the Ethiopian information and communication technology development agency[79], the MINT [80], NISS[81] and INSA[82] are organs with key roles.

---

[74] Federal Democratic Republic of Ethiopia, (n 72).

[75] Established on Nov/2010 as a continuation of GTP 2005/6-2009/10.

[76] https://www.ethiotelecom.et/%e1%8b%a8%e1%8a%a2%e1%89%b5%e1%8b%ae-%e1%89%b4%e1%88%8c%e1%8a%ae%e1%88%9d-%e1%8b%a8%e1%88%a6%e1%88%b5%e1%89%b5-%e1%8b%93%e1%88%98%e1%89%b3%e1%89%b5-2013-2015-%e1%88%b5%e1%89%b5%e1%88%ab%e1%89%b4/, last accessed 25/09/2020, 12:12PM.

[77] Ibid.

[78] Government Regulator for Phone and Internet Networks Until 2010, Gives a Sole Provider License to Ethio telecom.

[79] EICTDA, as Autonomous in 2005 formulated the National ICT Policy in 2009 and handle the so called "Woredanet" Program.

[80] Overseeing the Implementation by Assuming the Mandates of ETA and EICTDA in 2010.

[81] With a Broad Mandate, takes the Lead for any Matters of National Security and Intelligence.

[82] It is established to "ensure the Security of Information and Information Infrastructure to Facilitate their use for the Implementation of the Country's Peace, Democratization, Good governance, and Development Programs," which is taking more responsibilities as the Telecom Sector Grows up.

3.1. TELECOM FRAUD OFFENCES PROCLAMATION

After several preceding efforts that the government has made to regulate and administer the telecommunications industry, it has also enacted the Telecom Fraud Offences Proclamation No. 761/2012. As the objectives refers in the preamble, it aims at; ensuring the sector is implementing peace, democratization and development in the country, recognizing telecom fraud threat on the national security, safeguard national security and bridging the legal gaps.[83]

As per the interview with Ms. Mignot Zenebe,[84] FGAP, there are few cases repetitively appeared in reference to some provisions of the Telecom Fraud Offences Proclamation. As to her survey[85] 75% of cases in the last three years are based on 'bypass fraud', 12.5% of the cases are importation of telecom equipment without license and the remaining 6.25% is with regard of illegal importation of telecom equipment.

VoIP service is also the other frequently noticed fraud act committed in this regard even if it's not as such shown in the above statistics.

Opposing Article 3 of the Telecom Fraud Offences Proclamation, there are illegal usages of telecom equipment without having prior license from the authorized organ. Having these products by itself is criminalized in the proclamation also they had a great role for the execution of the offence.[86] In addition short message fraud is also spreading so fast following high number of mobile subscribers by sending false lottery messages for the customers and persuading them to send money for the inexistent situation. Since this offence is done through the government infrastructure, people may lose trust on the system which brought a negative impact.

There are also some acts stated in the proclamation but committed severally. Call back crime which means that distributing numbers in cheap price produced by foreign companies but works

[83] The Telecom Fraud Offence Proclamation (n 9), Preamble.

[84] Interview with Ms. Mignot Zenebe, Federal Attorney General Prosecutor, Organized and Trans Boundary Crimes Directorate, held on, 26 October 2020, 12:30 PM.

[85] Observance of the FGAP, based on the Assessment made on Cases Brought to the Unit, August 2019.

[86] Ibid.

in the country's telecom infrastructure, SIM Card cloning, Premium rate fraud are some of the crimes committed in this pattern.[87]

The proclamation missed some fraud acts to criminalize but they are still existing problems. The first missing point is that failure to state issues concerning sim card related offences which are broadly seen now helping for the execution of bypass, call termination or/ and sim box frauds. As the police information indicates most of sim cards found in the country sold without registration and such crimes are in most cases found without criminal liabilities.[88]

3.2. REASONS FOR THE SPREAD OF TELECOM FRAUDS IN ETHIOPIA

Even if we can't say that the Telecom Fraud Offences Proclamation is sufficient enough to cover all the crimes relating to telecommunications, is has significant role in combating most of the crimes.[89] Even though the convergence of the telecom industry and the technology advancements bring a better life, it also pave the way for the criminals since its getting more complicated.[90] In other words every updates in the telecom industry and the way they reach to users is so fast even up to importing illegal equipment under cover of the licensed materials by the customs authority.[91]

3.2.1. LACK OF COORDINATION

As to Chief Sergeant Tadele Wubetu asserts that, many of the current telecom fraud crimes are committed from neighboring states which use the countries sim card and telecom network with no fear of being prosecuted. As he said there are some places which the telecom network extends up to 100/200 meters from the borders into other country. In this instance the criminals use the Ethiopian sim cards, gateways and Ethio telecom's infrastructure to commit telecom fraud for their benefit that may create a big loss in the country hoping that the Ethiopian polices never pass the border and caught them being there an issue of jurisdiction.[92] Some of the crimes like call

[87] Ibid.

[88] Interview with Chief Sergeant Tadele Wubetu, (n 10).

[89] Ibid.

[90] Observance of FGAP, (n 85).

[91] Ibid.

[92] Interview with Chief Sergeant Tadele Wubetu, (n 10).

back and VoIP services are not prohibited in some countries which create a safe zone for the criminals to cause the attack.[93]

In other words, even if most of the telecom fraud crimes are provided in the proclamation with high penalty rates, there is still an exponential growth of telecom crimes due to the dynamic and complex nature of the information technology and telecom industry as well.

3.2.2. LACK OF PROPER ATTENTION

The severity of the crime and its loss on the economy of the country is not acknowledged by many organs previously that the telecom fraud crime has not got the proper attention. This plays its own role for the spread of the telecom fraud crimes. Even if some efforts are taken by the government which is appreciated, it's not there yet in both institutional setups and regulatory frameworks.

3.2.3. LACK OF ADEQUATE TECHNOLOGY

Telecom fraud crimes (for instance bypass fraud) are not the same with ordinary offline crimes which the police cannot arrest the criminal just by a regular search and seizure. It rather requires advanced technology and trained man power with intelligence techniques. Currently the NISS and INSA are conducting an operation in collaboration with the police whenever necessary. There are some challenges in conducting this task such as; the machines used for the crime are currently not becoming easily accessible for the system, the system may show wide potential areas while tracing the crime scene which makes the duty complex, shortage of sim cards and telephones used for the purpose of the operation, interruption of system power and the like.

The telecom fraud crime which exists in different forms time to time cannot be exhausted on a certain list to regulate and to put a certain legal measures to prevent the telecom industry by taking harsh measures. It rather needs to be technological friendly to cope up with recent progress in conjunction with legal frame works. We need to have comprehensive legal provisions which comply with the nature of the crime to give the legal stipulation a long-lasting effect. Unlike the other offline crimes we don't have to use a closed or exhaustive list of crimes and penalty rates to that of the online crimes, in this case the telecom fraud offences proclamation. It

[93] Survey, Telecom Fraud Offences Assessment, INSA, Feb. 2016, p.17

is because that a certain act may be outdated and replaced by another act which is not considered as a crime or it may appear as a high crime content/ tool after some time later. So it's difficult to determine online crimes and way of their execution since the technology is so dynamic.

Some circumstances which hinder investigation are: difficulty of identifying the criminals, sending of blocked risk area numbers, insufficient tele data of latitude and longitude and availability of many false positives.[94]

3.2.4. TEMPORARY OPERATIONS

The other problem is despite the frequency incidents of telecom fraud crime, operations are not done consistently due to different factors. This affect the prevention and containment of the crime since the criminals are getting much economic benefits to upgrade their techniques and strategies supported by advanced technologies. They changed their places and hide for some time severally while suspecting they are under surveillance and then resume their action with new setups. This problem plays its own role in the spread of telecom fraud offences.

With respect to coordination there is failure to conduct fast operation on identified points, lack of attention by the stakeholders being busy by their regular works are among the factors even if the law expect the 'the technical task force' to take place.

In order to take fast response to the crimes the stakeholders should be able to cooperate due diligently. Ethio telecom taking the lions share in this regard to take immediate action wherever there is a risk including blocking sim cards which are found in doing illegal activity. Concerning the calculation of risks the NISS and INSA take the responsibility in this regard. The next phase and power goes to the police who are mandated to investigate and analyze both document evidence and witness's testimony. The federal general attorney prosecutor then took the case to the court by instituting a file after examining the investigation. This kind of collaboration is very essential to combat the distribution of telecom fraud crime which is not conducting by the partakers regularly.

[94] Interview with Mr. Gemechu Merera, Expert, Ethio Telecom, Legal Affairs Directorate, held on Nov. 09/2020, 5:00 AM.

3.2.5. LACK OF SUFICIENT LEGAL FRAMEWORK

As we have seen above the Telecom Fraud Offences Proclamation has its own drawbacks starting from giving vague and ambiguous definitions to the fraud acts up to the lack of clarity of determining and over/miscalculating penalties for a certain crime act. The discrepancies with another law and the unpreparedness to new events like the proposed telecom privatization make the existing law unfit for the overall situation.

3.3. OVERLAPS BETWEEN THE TELECOM FRAUD OFFENCES AND COMPUTER CRIME PROCLAMATION

The Computer Crime Proclamation No. 958//2008 is in fact enacted in 2016 after the Telecom Fraud Offences Proclamation promulgated. The computer crime proclamation among other objectives it also aimed at ensuring the national security since cybercrime becomes a threat for national interest beyond its economic implication.

The Computer Crime Proclamation has four core elements in its content; 'crimes against computer system and data', 'computer-related forgery', 'fraud and theft', 'illegal content data' and 'miscellaneous computer offences'.[95]

Whereas the Telecom Fraud Proclamation regulates offences related with telecommunication services, products/equipment and also telecom network.

The need for and use of modern built in computer accessories like software and microchips to commit telecom offences seems to necessitate the enactment of Computer Crime Proclamation.

In fact the Telecom Fraud Offences Proclamation is the predecessor of the latter while the latter should ensure there is no discrepancy between the two. As we can see from some practical cases and examining the provisions in the two laws, there are similar definition for a certain act, double criminalization and different level of penalties which paves the way for violation and abuse.

There is a single provision which clearly repealed by Art 5 offences related to interception and access of the Telecom Fraud Offences Proclamation that stated under Article 45 of the Computer Crime Proclamation.

[95] Computer Crime Proclamation, 2016, Fed. Neg. Gaz, Proc. No. 958/2016, year 22, No.83.

The first discrepancy is though, Article 2(1) which defines the telecom services which includes the internet and data communication. It is better to remember here that both the internet service and data communication are hosted by computer networks.

This is because as it is stated under Article 2(1) of the Computer Crime Proclamation, '…..*computer crime means a) a crime committed against a computer, computer system, computer data or computer network…'* which also include acts against/by internet and data communication it may create a confusion as to referring which law when instituting a suit.

The other clash between the two laws is that there is similarity on the definitions of Article 2(2) of the Telecom Fraud Offences and Article 2(3) of the Computer Crime Proclamation while defining "telecom equipment" and "computer or computer system". The Telecom Fraud Offences Proclamation Article 2(2) says telecom equipment includes *its accessory and software* and the Computer Crime Proclamation also include these in its part. Here arises a big question on the importance of provisions of penalty rates laid for the telecom offences under the telecom fraud proclamation which are stated more comprehensively on the Computer Crime Proclamation.[96]

In addition to Article 3(2) of the Telecom Fraud Offences Proclamation which prohibits unauthorized importation, production, assembly of telecom equipment, the Computer Crime Proclamation puts under its Article 7(2) illegal access, interception, offers for sale, etc on the acts stated under Arts.3-6 of the same with similar stipulation. We can infer from this that even if both laws talk about same acts, they use different characterization to criminalize the same act. When the telecom fraud criminalizes accessing any telecom equipment without authorization, the Computer Crime Proclamation doesn't focus on just having the equipment rather prohibits using it to commit acts stated under the Articles 3-6.[97]

There is also a discrepancy under Article 6(1) of Telecom Fraud Offences and Article 14 of the Computer Crime Proclamation. As per Article 6, using telecom equipment or networks to commit acts anything related with the Anti- terrorism law, and any other acts punishable by law

[96] Interview with Mr. Million Haile Michael, Deputy Director, Legal Affairs Directorate, INSA, held on 30 October 2020, at 12:41 PM.

[97] Computer Crime Proclamation, (n 95).

are punishable when Article 14 of the later makes any violent content against public security and people punishable. But when we notice that the telecom equipment and network stated under Art. 6 of the Telecom Fraud Offences Proclamation are all the same with the computer system and network stated under the Computer Crime Proclamation; what we realize here is that just a duplication of laws.

By the same token, the Telecom Fraud Offences Proclamation criminalizes using telecom services and infrastructures for illegal purpose, which we can see that it's also considered as a computer crime as per Arts. 12- 15 of the Computer Crime Proclamation. The definition part of the Computer Crime Proclamation stated the telecom equipment provided by the telecom operator like, fixed line telephones, mobile phones, internet modems, routers are considered as computers. Similarly, telecom services like phone call, fax service, internet are provided to the customers by using computer networks. Any crimes committed by using these equipment and services are also computer crimes as per Art.2 (b) and (c) of the Computer Crime Proclamation. This makes a confusion in choosing the appropriate law for the trial since it is possible to commit crimes listed under Arts. 3 – 8, 10(1), 12 and 15 with same existing infrastructures. It is because one crime is treated differently in the two proclamations. [98]

The telecom infrastructure includes computer networks, which make stipulations of Art 7 of the Telecom Fraud Offences Proclamation and Arts.9 and 10(2) of the Computer Crime Proclamation similar. Article 7 of the Telecom Fraud Offences states offences related to fraud of service charge is a crime. This has also addressed in Art.9 and 10(2) stating that computer related forgery for oneself or for the interest of third parties is punishable which again makes the importance of two provisions for same act meaningless.[99]

Finally, regarding the procedures of investigation of telecom fraud offences,[100] the Telecom Fraud offences Proclamation follows same procedures in both its types and ways with that of the

[98] Ibid, Telecom Fraud Offences Proclamation, (n 9).

[99] As to me this should be considered on the computer crime proclamation since it's enacted after the telecom fraud proclamation, it must recognize and leave provisions for same offences to the telecom fraud proclamation. As there are also some complaints on the computer crime proclamation too, this must be one aspect for a revision if there is any proposed.

[100] Telecom Fraud Offences Proclamation, (n 9), Arts.14- 16.

Computer Crime Proclamation as it is stated under the Article 21 and the following of same. This is a serious concern when a case brought to the law in violation of Telecom Fraud Offences proclamation to choose which law be applied while conducting an investigation.[101] It must be clearly stated whether the provisions of the computer crime proclamation repeal similar provisions of the Telecom Fraud Offences Proclamation or if they still remain in force.[102]

3.4. GAPS IN SOME PROVISIONS AND PRACTICAL CHALLENGES OF THE TELECOM FRAUD OFFENCES PROCLAMATION

3.4.1. LIMITED AWARENESS OF THE JUDICIARY

The convergence of telecommunication and the internet brings a challenge in combating the fraud and fraudster since it is getting more complicated through time to time. This makes the prevention and control of the telecom fraud very difficult while the justice organs have limited awareness especially in this new technological field.[103]

As there is limited number of experts in the Judiciary on this area, the researcher even couldn't get judges to conduct an interview while they are frequently changing benches and there was no one around in the time of data collection who gets a training and had an experience of entertaining cases on telecom fraud offences proclamation.[104]

This creates a gap in the implementation of the law while bringing the case to the court. For instance, in most cases when the prosecutor institute a suit referring to Article 9, offence related to illegal telecom operators, it should be consolidated with Article 3 of the same law which is missed almost in every cases instituted to date.[105] This creates a gap in the implementation of the

[101] Interview with Chief Sergeant Tadele Wubetu, (n 10).

[102] Interview with Ms. Mignot Zenebe, (n 84).

[103] Interview with Chief Sergeant Tadele Wubetu, (n 10).

Chief Sergeant Tadele said there was only limited number of trainings he remembered they have got from INSA and Ethio Telecom in his 12 years of experience. They struggle by themselves as they keep getting the exposure to the cases and in the process of the investigation and the trial procedure.

[104] The police and Prosecutor were fortunately among the long-stayed experts on the area which they claim they got most of the knowledge from the exposure and, they had trainings from INSA.

[105] An Excel Sheet, a Summary of Case Reports tried in Reference with the Telecom Fraud Proclamation shows more than 10 cases have the same problem.

law that the suspect could be accused only in single provision while the act actually results in infringement of two provisions which seems out of the ambit of the law.

3.4.2. TRANSNATIONAL NATURE OF THE CRIME: as we said that the telecom fraud crime has universal nature which help the actor/s to execute the act from anywhere/to anywhere in the world. This again remains a challenge for the executive organ to bring the criminals to the national courts since the jurisdictional issue may appear inevitably.[106] There are many bypass frauds committed in Ethiopia from neighboring countries using the Ethiopian sim cards but couldn't easily been investigated because of jurisdictional issues. Tog-Wujale of Somali land claimed as a state hosting up to 50% telecom fraud crimes[107]committed against Ethiopia, is a potential hub of criminals targeting our country to commit crimes like bypass frauds as Ms. Mignot, FGAP has pointed it out.

3.4.3. DISPARITY OF LEGAL FRAMEWORKS: regulation of telecom fraud varies from country to country. A certain telecom fraud act could be an offence in one country but not in others. For example, a call back service is not prohibited in many other countries while it is aggravated crime punishable with rigorous imprisonment in our country.[108] This creates a fertile environment for the fraudsters to attack by residing in a place where such acts are not criminalized. It also makes the effort to cooperate with other countries difficult for joint prevention and control since there would be no uniformity in regulating telecom fraud crimes.[109]

3.4.4. LACK OF COHERENCE AND CLARITY OF LANGUAGE: there are some terms in this proclamation that are vague which may create confusions not only for the lay person but also for the expert of the area. Some terms should have been put in equivalent Amharic term or explaining the idea in clear manner in the definition part of the proclamation which deemed as very crucial for a certain law. Besides, there are some terms that cause a long debate while a case brought to the court.

---

[106] Interview with Chief Sergeant Tadele Wubetu, (n 10).

[107] Observance of FGAP, (n 85).

[108] Telecom Fraud Offence Proclamation, (n 9), Article 8 (1).

[109] Interview with Ms. Mignot, (n 84).

3.4.5. OFFENCES RELATED TO ILLEGAL TELECOM OPERATORS: accused persons usually defend themselves that the law prohibit only leaving aside the governments infrastructure by alleging that they use the same infrastructure for their act not bypassing as its referred in Article 9(b) as: *'bypass the telecom infrastructure established by the telecom service provider….'*

This has been a cause for a debate between the plaintiff and the prosecutor in the court which an equivalent definition for the term is needed to solve this problem.[110]

3.4.6. FAILURE TO DEFINE TELECOM OPERATOR: the other controversial issue in the implementation of this proclamation is that even if the term 'telecom operator' stated in the substance part of the law, it hasn't been defined what does it mean and what services are being provided by it.[111] This has also been an issue for argument since the enactment of the law.

The Telecom Fraud Offences Proclamation stated that the law deems responsible the operators for their omission. Chief Sergeant Tadele in his other insightful critics of the law, it shouldn't put **'**operators' the only responsible organ for telecom fraud acts. "Practically speaking operators are not found in the crime scene in most cases even not in the country." There are different telecom equipment we caught on the hand of individuals even sometimes without committing another fraud action as he shares his experience. He told that they may catch suspects in borders having such equipment while they left without power to arrest them since there is no law supports them to do so. "These days the criminals are smarter than us that they never let us to arrest them simply for founded with the equipment. This is the major gap of the law that left the illegal access and possession of such items aside. We strive to find other stipulations to make them responsible for not letting them go since we can at least suspect they will never use such equipment for personal use and for legal purposes", Chief Sergeant Tadele said.

[110] **'ወደ ጎን በመተው'** የሚለውን ለትርጉም የተጋለጠ ሀረግ ወስደው ባለው መሰረተ ልማት መጠቀማቸውን በማመን ህጉ የሚከለክለው አዲስ መሰረተ ልማት መዘርጋት መሆኑን ይህንኑ አንቀፅ ጠቅሰው ይከራከራሉ፡፡

[111] Chief Sergeant Tadele explains that "we face a problem from the suspects argue that they just have the equipment with no intention and/act of telecom fraud while they caught hand red with the items alleging that they can't be deemed as operators in which the law doesn't include them in Article 3(1) of the proclamation which has more penalty."

3.4.7. OFFENCES RELATED TO TELECOM EQUIPMENT: most cases instituted recently are referred the provisions of provisions of telecom infrastructure while the exhibit shows assembling of telecom equipment which hasn't been mentioned in the definition at all.[112]

But as it can be seen from several cases brought to the court, it raises a question whether the exhibits brought by the police show the offence of constructing a telecom infrastructure or assembling telecom equipment. Well, in most of the time there is still a confusion in this regard.

The controversial issue here is that the law under Art. 3(3) stated that as per the same provision it is prohibited to have any telecom equipment without the permission of the ministry (MINT).

The very aim of this provision was to fill the gap under the repealed telecommunications law, i.e. proclamation No. 49/89 which lists out type approvals that are allowed to be found and possess by a person and states that any additional license for other equipment will be provided in public notice when it deems necessary. This doesn't match with the current technological convergence which also paves the way for the monopolization of telecom services by the government. When we come to our recent law as it stated in the above provision, it shows same problem again since the listing of type approvals given to MINT which actually never done yet. The reason for this might be the nature of the technological advancement which unable the regulator to determine which items are legal and need to be handled only by the government and which are let for the public. Thus this makes a person liable only for having certain telecom equipment whether it's useful or harmful for the public security without a prior permission of the ministry.

I was wondering to know whether my cell phone is among the permitted item or not which I raise the question to Mr. Gemechu Merera, a legal expert at Ethio Telecom who doesn't seem like the irony and answers that "we don't need to take it such strictly since the intention of the legislator is clear that it's mainly to protect the national interest and the equipment found should be harmful for the public security and/or create an economic loss to the country. Otherwise the Government is striving to provide a quality service for mobile and internet to let the people stay more connected."[113]

[112] Interview with Ms. Mignot Zenebe, (n 84).

[113] Interview with Mr. Gemechu Merera, (n 94).

Well, it poses another question, if it's about connecting people what makes owning a satellite in one's house illegal as long as there is no legal framework clearly stating that.

3.4.8. CRIMES RELATED WITH PROVIDING UNAUTHORIZED TELECOM SERVICES: as per Article 4 of the Telecom Fraud Offences Proclamation a person found providing telecom services without authorization may be punishable from 7 up to 15 years of imprisonment. The term telecom service as the law refers it includes services starting from a resale up to being an operator which seems not fair to treat all of them together while imposing a penalty.[114]

In fact this provision needs to be seen in conjunction with Art. 9 which states offences related to illegal telecom operators since unauthorized services are obviously provided by illegal operators or it should be clearly stated if the case is different.

3.4.9. OFFENCES RELATED TO CALL BACK SERVICES: besides its technical meaning in the definition, the call back defined as it is equivalent with a bypass fraud or call termination act. The last phrase of the definition says that a call back means hosting international calls as if they are incoming local calls, which exactly refer to bypass or call termination crimes.[115]

In addition, as we can infer from Art. 8(2) of the proclamation, every person using the service intentionally or negligently will be liable for punishment. This seems not fair and unwise to lay a responsibility on a lay man in which the technological penetration of our country is very infant that the community's level of awareness about their acts specially when using a computer and computer systems in every aspect is very low.[116]

3.4.10. VoIP[117]: giving a phone call and fax service using the internet is clearly prohibited under the Telecom Fraud Offences Proclamation (Art.10 (3). But it's not yet clear that whether all

[114] Interview with Million Haile Michael, (n 96).

[115] Ibid, Interview with Ms. Mignot, (n 84).

[116] Interview with Million Hailemichael, (n 96).

[117] As per the ITU's definition VoIP means making calls through internet protocols which reach through different internet networks. VoIP can be conducted in two ways; the first voice call is that transmitted through public internet line while the other one is made through private network (private IP). The difference between the two

types of VoIP services are prohibited by this law or not. There are three perspectives that the judiciary put as various ways of interpreting this provision.[118] The first one is that the law lays a restriction on every kind of VoIP service and whosoever uses the service will also be punishable but not using for personal use only. This means that no commercial activities are allowed in this provision except for personal use only. The second perspective tries to put a distinction between hosting a phone call and transferring voice call through the internet. It's said that VoIP is different because it's conducting a voice call from the internet to the fixed line or it could be from fixed line to the internet. While in a phone call it means that making a call from internet to the fixed line or vice versa but it never includes internet to internet, i.e., skype, viber, etc calls. As per this perspective only calls made from the internet to fixed line are prohibited. The last perspective pinpoints that VoIP means any kind of internet-based calls which the law also indicates the whole prohibition of it. And individuals by any means use VoIP will be liable for their misdeeds.[119]

3.4.11. ETHIOPIA and VoIP: even if this law addresses the VoIP services**,** it however lacks some clarity both for the executive organ and the judiciary which still need some clarification regarding creating reliability and builds trust in the public. It is also important to understand the intention of the legislator in order to have a clear understanding of the law concerning VoIP in Ethiopia. The intention of the legislator seems that the law intends to prohibit the calls that are made from internet to fixed lines but not that are made from internet to the internet. The term "telephone call" here indicates the notion of this assumption.[120] Nevertheless, the proclamation doesn't put clear definition for the two terms and couldn't be sure the above intention is really the legislators'. Even though, the definition part has in its meaning that 'internet service means also a telecom service, it doesn't mean that it includes VoIP, fixed line or mobile phones networks. Phone calls are ordinary calls made through normal telephone line (PSTN) whereas internet calls are all VoIP's. Hence the law shows us as every VoIP's are prohibited in Ethiopia

---

calls is that clarity of voice calls in which the public internet lines are mostly focus on the quantity of short messages even if this is believed that will be updated by the technological advancements.

[118] Survey (n 93).

[119] Ibid.

[120] Telecom Fraud Offence Proclamation, (n 9), Art.10 (3).

which the intention of the legislators and what the law says are different.[121] Having a close scrutiny of the legislator's intention, it's better to understand that the law want to have a control on operating VoIP rather banning all the services either putting requirements or requires for a prior licenses from service providers, maybe with some restrictions.

Ethio Telecom banned some telecom services severally by claiming the national security and/or following the government's policy direction on the area.[122] VoIP and call back services are among these sudden restrictions.

The government should be careful in this regard while hosting private companies in the telecom sector. The private companies are inevitably seeking to provide more services as much as they can and maximize their profit margin which these services be among their menu.[123] If restrictions are somehow be loosen in any way for the new comers, it should be clearly shown in the law with all prerequisites, exceptions, criminal liabilities and also enforcement mechanisms so that it can be duly emphasized.[124]

3.4.12. REGISTRATION AND DISTRIBUTION OF SIM CARDS: the other practical challenge has been noticed that the uncontrolled distribution of SIM cards and unregulated transfer/sale occurred due to unavailability of regulatory frameworks. Unregistered SIM cards are used to commit crimes such as sim box frauds which creates big economic loss in the telecom industry.

The telecom fraud offences proclamation said nothing about taking SIM cards and airtime voucher cards abroad. The bulk availability of these items helps the offenders in outside to commit telecom crimes.[125]

Based on the interview with Chief Sergeant Tadele Wubetu, it is almost beyond their capacity to control and handle the issues relating with SIM cards. As Chief Sergeant Tadele describes,

[121] The notion of the 'intention of the legislator' grasped from the commentary, the preamble and by analyzing the spirit of the provisions of the telecom fraud proclamation.

[122] Survey, (n 93).

[123] Ibid.

[124] Interview with Gemechu, (n 94).

[125] Survey (n 93).

almost all cases brought to the police in relation to SIM cards have not been registered. He said that there is a guideline[126] which Ethio telecom had tried to govern the retail SIM card distributors like Post offices and Tele centers are required to report to Ethio Telecom which is established by internal guideline that Ethio Telecom oblige the retailers that they are expecting to report their sales in specified amount of time, to have profiles of the buyers registering the SIM cards by their name and so on. But there is no enforcement mechanism put on the guideline when the distributors fail to do so. It has been said that it doesn't brought major change. Chief surgeon Tadele added that there is no even a special license required for SIM card distribution, an owner of mini kiosks or stores can have it with their existing business license.[127] As to chief sergeant Tadele's observation, there is no clear position between the Ethio Telecom staffs. One side supports the bulk sell of SIM cards by any means possible thinking only just the level of number of subscribers towards their profit and the other side of argument from the security perspective, claims that it needs some regulation including strict registration manuals.[128]

Even if the law has nothing about these issue Ethio telecom try to manage it by a sales contract with the distributors obliging them not to sell SIM cards without registering personal profiles of buyers which in fact hasn't been well implemented so that it doesn't brought major change.[129] And, the fact that there is huge difference in local and international call tariffs attracts the fraudsters to commit bypass fraud using the local SIM cards which result in a big economic loss at the telecom market.[130]

There are again two perspectives about criminalizing these acts; first one is that Ethio Telecom can control this technically so there is no need of criminal stipulation fearing that distributors may abstain from selling and distributing those items not to bear the penalties.[131] On the other

[126] Guideline prepared by Ethio Telecom for SIM card distribution, 2009 EC. Stating that any SIM card sale should be registered, and no one can have more than 5 SIM cards.

[127] As to Chief Surgeant Tadele describes he never seen cases with registered Sim cards and distributors with specific license among the crimes they have investigated.

[128] He said this remains an issue between the sales department and legal/security unit of the organization.

[129] Interview with Gemechu Merera, (n 94).

[130] Ibid.

[131] In the current situation selling and/distributing SIM cards are not as such profitable, so it may not be worth scarifying.

hand, the second position states that technical and technological solutions may not be enough without harsh legal frameworks to combat this crime.[132]

The other point raised here by Ms. Mignot Zenebe, FGAP, is that there is still a problem in failing to give a type approval for SIM cards as a telecom equipment as she alleges it is missing the essence of the definition given for 'telecom equipment' in the proclamation[133] which mostly make them lose a case since the court usually excludes SIM cards from telecom equipment. Even if the law gives the mandate to the technology and innovation minister to prepare such list which the ministry had nothing about the list and standards of type approvals and excludes SIM cards from the definition of 'telecom equipment'. This is defying the ambit of the definition of the proclamation while it's saying '*…anything used for telecom services…accessories…'* and paves the way for the criminals by giving them to get a loophole for their fraud actions.

3.4.13. FAILURE TO PROVIDE LIST OF TYPE APPROVALS AND TECHNICAL STANDARDS

The telecom fraud proclamation under its Article 3(3) states that the Ministry (Ministry of science and technology) *shall prescribe types of telecom equipment the manufacturing, assembling, importation, sale or the use of which may not require permits, and set their technical standards.* The law also provides that any misdeeds in violation of this provision without authorization shall be punishable with 1-4 years of imprisonment and fine from 10,000-40000 birr.

We can raise two critical issues here, the first one is even if the law give the mandate to the ministry to prepare a list of technical standards and type approvals, there is no such list prepared since the enactment of the law up to the date of this research is conducted. These results a practical challenge since the judiciary obliged to require a type approval from the ministry in a case by case basis.[134] As Ms. Mignot pointed out this challenge affects the implementation of the law and violates the right of people mentioning a case brought to her by alleging the fact that a

[132] Interview with Mr.Million Hailemichael, (n 96).

[133] Telecom Fraud Proclamation, (n 9), Article 2(2) states that, 'telecom equipment' means any apparatus used or intended to be used for telecom service; and includes its accessories and software.

[134] Interview with Ms. Mignot Zenebe, (n 84).

person arrested while found with TP- LINK device which anybody can buy and use once it's imported. So, it's not legal to accuse someone only for the fact that he holds such devices defying the basic criminal law principle of no law no crime. [135]

As per an interview made with the federal public prosecutor, the issue of type approval is one of some practical challenges that affects a court proceeding. For instance Ms. Mignot raised that even if the Telecom Fraud Proclamation under states[136] that the Ministry of Innovation and Technology has a duty to list out and prepare technical standard for telecom equipment that would be assembled, imported for sale or for any use without prior notice of the authority, but it has done nothing yet for the past more than seven years.[137] Consequently, the prosecutors forced to request list approval for each and every equipment that creates inconvenience in the course of examination of cases.[138] She alleges a new fact that INSA is currently trying to list out equipment in coordination with Customs at the bole international Airport while the equipment arriving in the country even if it is not exhausting enough. But here the question is first of all INSA as we know is mandated to regulate the security aspects of information technology equipment which also it is doing of course for the security aspect of the importing equipment. Secondly even if it's good to make the clearance on arrival, it still creates a confusion on the justice organ as well as the community since there are no black list nor white list.[139] According to the police, there are some devices imported even directly in the airport, border customs, by post

[135] Ibid.

[136] Telecom Fraud Proclamation, (n 9), Article 3(3).

[137] Ms. Mignot speaks witnessing the survey they made on the Telecom Fraud Offences Proclamation; she didn't find any progress on this regard from its enactment of 2004 -2011.

[138] A certain case brought to the court in reference to this provision that wrongly instituted a file against one person found having an instrument called a 'TP-LINK' which actually helps for telecom service. Ms. Mignot added that even if this device needs a permission for entrance for the sake of standardization, but it may be found in the market without restriction. Ms. Mignot said since there is no provision for minimum number of SIM cards specified, there are many instances that a person with hundreds and thousands of SIM cards that had let free because of lack of specific law knowing that they could be used for the telecom fraud crimes.

[139] Observance of the FGAP, (n 85).

and through different mechanisms while some legal materials are caught for arrest due to the absence of such regulatory frameworks. [140]

There is even an incident that the former customs authority sold the TP-LINK devices to the public with an open bid which are caught at contraband and confiscated by the Customs authority.[141]

There was some move from the government to register mobile apparatus, but it is said suspended now. Mr. Gemechu points out that it seems in some extent helps to national security, to control the network quality and to protect the local telecom operators from illegal products. Such act of registration of mobile apparatus would also help to prevent illegal telecom products not to enter into the country which save the manufacturers and also the government from financial loss.[142] Products with no standard usually create high connection pressure on the telecom network which also affects health and some related issues.[143] Mr. Gemechu puts that the registration of mobile apparatus has been suspended because of the operating system came up with a limitation that the original owner of the phone had been caught while tracing in the commission of the crime since the identification number refers to him while the phone is stolen and used by another person.

The list of type approval is though very important that could in advance notify any party who intends to import any telecom equipment before arrived in the country. This could be done simply by uploading the lists via the websites of customs of airline, mail expresses, checking points of different parts of the country before the illegal equipment reaches on the hand of the criminals.[144]

3.4.14. IMPROPER CALCULATION OF PENALTIES: the telecom fraud offences proclamation stated under its penalty clause that a person should be penalized with fine up to ten times of his economic gain from a certain illegal activity when he found guilty.[145] It is not

[140] Interview with Chief Sergeant Tadele, (n 10).

[141] Observance of the FGAP, (n 85)

[142] Interview with Million, (n 96).

[143] Interview with Mr. Gemechu Merera, (n 94).

[144] In most countries the websites of the airlines, customs authorities and the like have list of type approvals since anybody can first check before arrival.

[145] Telecom Fraud Offence Proclamation, (n 9), Arts. 8 (1), 9 (1) (a) (b).

possible to easily identify the amount of the profit the criminals gained rather it is only the estimated amount of the government's loss that can be calculated. As per the recent technological examination tool, it mostly retain maximum of six months of backlog files. In this regard there are some cases decided very low since the discretion of the judges is based on their knowledge and evaluation. In contrast, there may be also aggravated decision not understanding the difference of government loss and profit gained by the criminals. Ms. Mignot remembers a case which accused for causing a loss of 40 million birr to the government and the court simply decides on the criminal to pay a damage ten times of the above amount i.e. 400 million which seems never be executed due to many practical reasons.[146]

This makes the court to pose a penalty rate on the criminal equivalent to the exact profit gained by the criminals. This leads the court to pass a decision in a base of 'undetermined gain' which practically didn't match with the damage. In contrast with this there may be an exaggerated decision by the court while the judge arbitrary multiplies the loss of the government considering it is gained by the criminals.

3.5. TELECOM LIBERALIZATION AND ITS IMPACT ON TELECOM FRAUD OFFENCES LAW

After a long time monopoly, the Ethiopian Government decides to part privatize Ethio Telecom keeping 51% for itself and to transfer the rest 49% to private companies.[147]

The former Minister for Innovation and Technology, Dr Getahun Mekuria had once tweeted that he considers the move *"huge step."*[148] Ethio Telecom which is currently hosting larger number

[146] First of all, it's not the proper calculation since the system cannot show the profit gained by the actors. The other point is that in most cases the suspects are very poor even below the normal standard of life generating very low income. They are recruited due to their level of life as they confess by just told that they will receive a certain amount of money for their small contribution just as renting a house, connecting a device, popping up airtimes, checking the electricity and connection.

[147] https://www.theafricareport.com/39864/ethiopia-the-case-for-partial-privatization-of-ethio-telecom/

[148] Morris kiruga, in Nairobi, Ethiopia's liberalized telecom sector offers opportunity with glitches, theafricareport, posted on Tuesday, 18 June 2019 15:24, available at, https://www.theafricareport.com/14199/ethiopias-liberalised-telecom-sector-offers-opportunity-with-glitches/, last accessed 10/31/2020, 10:09PM.

of subscribers even more than the renowned African countries telecom companies[149], would likely be split into two. The Telco is one of Ethiopia's "commanding heights": state –owned enterprise that Prime Minister Abiy Ahmed is seeking to privatize either fully or partially.[150]

This reform on the telecom sector may bring its impact on the implementation and the fate of telecom fraud proclamation.[151]

Even though the government put a direction for Ethio Telecom to move on the next phase of the liberalization process there is not yet produced full and clear document which shows the whole procedure and the extent of privatizing. This may affect the current telecom fraud law in making some remarks on amendments or any other measures on the existing law.

The government as a regulatory measure enacted the communications service proclamation No 1148/2019 to establish the Ethiopian Communications Authority and to determine powers and functions thereof. Yet there are some issues that need a clear direction as to how some issues can be treated in the phenomenon.

3.6. COMMUNICATIONS SERVICE PROCLAMATION

The Communications Service Proclamation No. 1148.2019 aiming that establishing an independent institution in order to achieve the Government's policy of restructuring the telecommunications market and introducing competition.[152] This proclamation established the federal organ called Ethiopian Communications Authority /ECA/ also known as the Authority which is believed to accomplish its mandates and it is accountable to the Prime Minister.[153]

[149] It has been reported briefly surpassing the Nigerian MTN in number of subscribers in 2017.

[150] https://www.theafricareport.com/39864/ethiopia-the-case-for-partial-privatization-of-ethio-telecom/

[151] Interview with Million, (n 96).

[152] Communications Service Proclamation, 2019, Fed. Neg. Gaz, Proc. No. 1148/2019, Year, 25, No.82, Enacted to establish the Ethiopian Communications Authority.

[153] Id, Article 3. Prime Minister Abiy Ahmed once his discussion with Political Parties about Telecom liberalization, said that the government leave the accountability of the Authority directly to the Prime Minister because the government want to have a close eye on the procedures of the Telecom Privatization in order to prevent corruption and any other misdeeds.

The Ethiopian Communications Authority in its powers and responsibilities held activities with respect to telecommunications services, equipment, control the telecom operators and so on.[154]

The power to list type approvals and technical standards is now hand over to this authority based on the establishment proclamation. As the police raises a recent challenge that the authority is not preparing the intended list by claiming that they are not on their marks for proper activities while the ministry of innovation and technology also rejects any approval request by referring the new law.[155] This creates huge financial loss as well as becoming a threat for national security since the situation creates a room for the criminals to enter into the country freely since the police left idle to regulate the illegal equipment. Some individuals/entity could have obviously a secured communication using those materials since they are not pass through the proper security clearance and also may escape surveillances.[156]

The other point which needs further clarification with regard to type approvals is that there are two tasks one is about regulating the quality and security of the products. On the other hand, there is an effort to transform the technology as well as to increase the number of the customers. Thus, the government must create a middle ground for these contradictory issues in order to have space for both scenarios as they are equally useful for improved and adequate service.[157] For instance, the Kenyan law put pre conditions for import goods which states that any Kenyan citizen can have and there is a restriction on those imported goods not to be transferred to illegal activities by imposing penalties. This could be considered as a best practice in our system too.

The Communications Service Proclamation has also given power to the authority to issue regulation and directives to the implementation of the proclamation.[158]

[154] Communications Service Proclamation, (n 152), Article 6.

[155] Interview with Chief Sergeant Tadele Wubetu, (n 10).

[156] We are currently seeing cases that individuals are found using satellites in their houses, what are they really doing with such equipment? Is that just for satellite television channels?

[157] Interview with Chief Sergeant Tadele Wubetu, (n 10).

[158] Communications Service Proclamation, (n 152), Article 54.

3.6.1. DRAFT DIRECTIVES

Following this power, the authority has issued some directives such as sim card registration, networks inter connection, colocation, universal fund, universal access, lawful tariffs and other which are open for public consultations and stakeholders review.[159]

The authority has prepared different directives which most of them are now ahead of final approval stage to undertake the issues of telecom privatization thinking to have a better implementation while hosting private companies. Sim card registration, mobile number portability, national Roaming Directive, Universal Access and Service, Universal Fund regulation and directives are among the first legal documents prepared by the authority.

The Sim Card Registration Directive which is expected to solve the issues concerning the crimes committed by Sim Cards due to the fact that there is no a limited number of Sim cards which is allowed to be accessed by an individual and also there is no accurate registration rule followed by the retailers.

It has put some draft rules concerning the registration and regulation of administration of Sim Cards but it fails to incorporate the new trend that's virtual Sim Card in which exist recently. As to the police,[160] most of recent crimes of Sim box Fraud are committed by virtual sim cards.

A sim box fraud is becoming prominent as we have seen it above. It would be worse when the privatization take place. It is because it may create a big harm on the government and private sectors as well.[161] Ethiopia is becoming a fertile zone for sim box fraud due to the tariff difference between the local and international calls.[162] As to Mr. Million's opinion, Ethio Telecom in its first job done when the new management took place, i.e. the discount in local call tariffs, was not a good idea which he believes worsen the situation since it widen the gap between the two call tariffs.[163] In fact there is an argument that the tariffs are not as such wide

[159] https://eca.et/.

[160] Interview with Chief Sergeant Tadele Wubetu, (n 10).

[161] Ibid.

[162] Interview with Million, (n 96).

[163] The tariff change helps the criminals from abroad since their call reaches to the local customer via local network, they would pay in local tariffs while they take the difference with the international calls to themselves. We

since Ethio Telecom itself has a charge to pay to the international operators which itself buys the service from foreign companies.[164] Therefore, such kind of crimes obstacles the legal operators and the government to get proper advantage; it also hinders the customers not to get quality and adequate services.[165] As we can infer from the experience of Ghana, the operators are coordinating with the government to fight the crime though they are losing a lot.

Crimes committed against sim cards hadn't been acknowledged and get legal framework. There has been bulk distribution of sim cards and the guideline of sim card registration hasn't been properly implemented.[166] This issue must have a clear-cut framework that Ethio Telecom tends to sell many sim cards which having many distributors. Since the distributors are not encouraged by the profit the price for sim cards are very less, they would for sue leave the market. So, we need to have strong regulation on the distribution and registration of sim cards. It's also better to see if there is any technological tweaks that help to fix such kind of problems.

As to Mr. Gemechu's opinon, it's not enough even the directive imposed by Ethio Telecom implemented seriously since the criminals can go to several shops and buy many 'five' sim cards since there is no strong controlling mechanism. In addition, the guideline didn't put a liability clause to internal fraudsters when the staff of Ethio Telecom are repeatedly accused for participating in this crime.[167]

3.6.2. TELECOM INFRASTRUCTURE

A telecom infrastructure is one of the key infrastructures of the country in which the government invests huge investments even if there is still in adequate coverage. The current level of network penetration and diversified telecom services are leading to high demand of telecom infrastructure.

---

remember that Frehiwot Tamiru, CEO Ethio Telecom, take this among the first reform measures when she came to the office.

[164] Interview with Mr. Gemechu Merera, (n 94).

[165] Mr. Million believes that it is because duplication of non-standard products of Mobile Apparatus that the network getting Busy and out of service.

[166] Interview with Mr. Gemechu Merera, (n 94).

[167] Interview with Mr. Gemechu Merera, (n 94).

The newcomers who are expected to conduct a diversified telecom services are also expected to show high demand of the telecom infrastructure. The Ethiopian Communication Authority though is trying to address this issue in the co-location draft directive.

Ethio telecom in its preparation to host the entrance of the private telecom providers stated that additional investments are also deploying on telecom infrastructure.[168]

3.6.3. SYSTEM AUTOMATION

BANK FRAUD

Following the transition of many banking services via telecom networks and mobile phones, new crimes are born to abuse the technological advancement. Witnessing Mr. Gemechu Merera, there is a new fashion of crime which is called a 'bank fraud' committed using sim card cloning techniques. As he has explained, people first make a forgery of the identification card of a certain individual and using that fake identity they report to Ethio Telecom to get a substitution of sim card by claiming that the previous one is stolen. Then after having same number with the original's they went to the bank with a cheaque pretending that it's endorsed by the customer. Usually the bank calls to its customer to get a confirmation before paying a cheaque. The criminals here use this gap pretending as if they ordered the prescribed amount to the holder which the banks pay frequently with no further investigation. This can be caused mainly by the weak customer service and cyber security system of the banks which most services are now delivered on hand. Taking this change into account, most banks are automating their services using the internet and providing services through mobile phones which we hear here and there advertisements like paying of bills, booking air tickets, and different social services. Even if the government doesn't allow the coming private companies to undertake banking services yet,[169] it's better to be prepared for same and other challenges which inevitably would happen at some point in time.

[168] 3-yr-strategy-01-1.svg

[169] Ms. Frehiwot Tamiru, CEO, Ethio Telecom, while discussing about the procedures of liberalization to the public, said that the new private operators are not allowed to conduct banking services for the time being.

3.6.4. LICENSING

The other concern in this regard is that the share of local companies and citizens should be specified whether they can participate in this process or if it is only for foreigners. As it stands now there is no clear there is no clear direction put by the government. How many operators would involve, do the government make background checks of the companies both for the sake of national security and their profit making records as well?, is there any privilege for the government share or not and so on?

The Communications Service Proclamation govern functions and telecom business activities of the private companies strictly in which they would find a way using every loopholes of the law. There is no surprise that private companies would work mainly for maximizing their profits and they could also be a threat for information security. There is also an instance that they want to make sure they are protected by legal frameworks since they are also exposed to some threats and may be a victim while conducting the business. Therefore, had it been only the government as to the previous time, it wouldn't be as such an issue to safeguard the national security and balancing the economy in providing telecom services but now there is another story following the entrance of foreign private companies.[170]

[170] Interview with Mr.Gemechu Merera, (n 94).

CHAPTER FOUR

CONCLUSION AND RECOMMONDATIONS

4.1. CONCLUSION

As the telecommunication industry deploys more and more technological advancements and becoming the most prominent tool of communication throughout the world, Telecom fraud is now the fundamental problem of the sector.

Telecom fraud in its very essence means that an abuse of telecommunication services /equipment/ service frauds, bypassing and would also be using telecom networks for disseminating any illegal contents.

It could be expressed in different ways both with respect to types of telecom fraud and ways of execution of the crime. Contractual fraud, hacking fraud, technical fraud and procedural fraud are groups of telecom fraud. Bypass Fraud, Sim Box Fraud and private Branch Exchanges are among the types of telecom fraud crimes.

Due to its dynamic nature telecom fraud is becoming a tough task for both the legislator and executive body in order to control the crime effectively. It has a transboundary nature where it could be committed from anywhere and can target any body found in the whole world. Since the crime is committed from different parts of the world people may coordinate from different places to commit the fraud act. The complexity of the crime is also another feature of the telecom fraud crime. Since it could be committed from anywhere anonymously, it's hard to track the identity of the person participated in such act. Comparing the cost incurred at the commission of the crime, the execution is very cheap. That's one reason that the fraudsters choose it as a new trend.

The information technology era is very dynamic. Technological advancements are the typical feature of the telecom fraud crime. The technology bypasses easily a certain coping mechanism and updates itself consistently. This is in fact the biggest challenge for the legislators and the executive body as well since a certain law would be outdated after a short period of time of its enactment.

Different countries took different legal measures to combat the commission of telecom fraud crimes and its impacts on infrastructure and public security. The experiences taken from Kenya, Ghana, Egypt and Myanmar are some of the countries consulted in this paper for their best practices.

Some practical cases show that there are implementation gaps of the Telecom Fraud Proclamation as to which the practical challenges appear because of some provisions of the law. The problem emanates from the definition of terms, double criminalization, and failure of stating a legal provisions for a better prevention of the crime. The misrepresentation of call back service and bypass fraud is among the major gaps of the existing Telecom Fraud Offences Proclamation.

The call back service which is not well defined in the proclamation rather refers a call termination act, contradicts with the punishment clause of bypass fraud and made every person liable who even use the service unintentionally.

The concept of telecom privatization becomes another challenge to the existing situation and may also bring additional security threats in the telecom industry. The private operators who are expected to join the telecom market would be exposed to a cyber-attack/threat and also the problem would still be appeared from the other side since they could also be a potential threat who would bring a problem on the country's key infrastructure and public security as well.

Therefore, we could not say that we have a comprehensive legal framework to govern the Telecom Fraud Offences as to the prevention, proper criminalization, institutional setups and better implementation clauses. The current law doesn't comply with the technological advancement of the state of crime as it has a dynamic nature which the criminals keep upgrading their skills.

4.2. RECOMMONDATIONS

Based on the examination made towards the Telecom Fraud Offences Proclamation its implementation and practical challenges and gaps, the researcher strongly believe that the existing law needs a serious consideration to its amendment. The challenge comes from both the implementation gaps and facts which are missed to be included in the law.

But for the consideration of general reform there should be some specific changes regarding specific provisions and implementations. The following are some of the recommendations which the researcher believes very crucial;

- First some vague and ambiguous terms in the definition and other part of the proclamation needs a serious revision.
- Most of the problem faced by the police officers and the prosecutor is that lack of awareness/expertise which needs a consistent follow-ups and trainings.
- It's better to see the Telecom Fraud Offences in contrast with Computer Crime Proclamations for a better implementation either by merging or putting a clear demarcation between the two.
- The SIM card registration and determining maximum amount of SIM cards that can be found with one individual would have a great effect on the prevention and controlling the impact of telecom frauds. Thus, the new draft guideline should properly address this issue considering the virtual Sim Cards with strong and clear enforcement mechanisms.
- There is a mandate for listing type approvals which were gave to the Ministry of Innovation and Technology in the existing Telecom Fraud Offences Proclamation which it is now transferred to the Ethiopian Communications Authority. This gap is giving a room for the criminals that the relevant authority need to fulfill its responsibility as soon as possible.
- The Technical ask force should be formally established by authoritative organ and conduct activities as per the law.
- There have to be clear list of type approval considering the technological advancement and need to prepare a so called **'grey list'** which would be of the owners' risk that the customs may allow to enter to the country or not.

- The VoIP service should have been given a clear definition and it's better to legalize the usage of the service with normal internet fees since some of the telecom fraud offences are targeting to escape the expensive international call tariffs.
- Technological advancement also needs to have an emphasis in which we cannot attain a better implementation of cyber security generally unless we keep updating.
- Until consideration of amendment or otherwise of this law takes place, every partakers should fulfill their responsibility for better implementation of the existing law at least it may help to ease the problem until resolved.

BIBLIOGRAPHY

1. Legislation

1.1. National Legislation

- Computer Crime Proclamation, 2016, Proc. No. 958, Fed. Neg. Gaz., Year 22, no.83.
- FDRE Criminal Code of Ethiopia, 2004, Proc. No. 414.
- Telecom fraud Offence Proclamation, 2012, Proc. No. 761, Fed. Neg. Gaz., Year 18, no. 61.
- The Federal Democratic Republic of Ethiopia Criminal Justice Policy, Ministry of Justice, 2011, Amharic version.

1.2.International Instruments

- Egypt Telecommunication Regulation, 2003, Law No. 10.
- Egyptian Anti-Cybercrime Law, 2018, No. 175.
- Guidelines for the implementation and provision of VoIP Services, Communication Commission of Kenya, 2005.
- Kenya Information and Communications Act, Revised Edition 2012 [1998], Laws of Kenya, Chapter 411A.

2. Cases

- Federal General Attorney Prosecutor vs. Mohammed Abdulselam and Others, File No. 481/08, Dead Case.
- Federal General Attorney Prosecutor vs. Ziyad Mekuriya and others, File No. 480/08, Dead Case.
- Federal General Attorney Prosecutor vs. Tessema Hunde, File No. 003/09, Dead case.
- Federal General Attorney Prosecutor vs. Yesouf Hassen, File No. 190/08, Dead case.

3. Interview

- Interview with Mr. Gemechu Merera, Ethio Telecom, Legal Affairs Directorate, 9 November 2020.
- Interview with Million Hailemichael, Information Network Security Agency, Chief Cyber Law Expert, Deputy Director, 30 October 2020.
- Interview with Chief Sergeant Tadele Wubetu, Federal Police Crime Investigation, Financial and Property based Crimes Investigation Unit, Crimes

against Governmental Institutions Secretariat Office, Supervisor, 26 October 2020.

- Interview with Ms. Mignot Zenebe, Federal General Attorney, 26 October 2020.

4. Press Release

- Frehiwot Tamiru, CEO, Ethio Telecom, Address on her Presentation to business Startups about the Telecom Privatization…/2020.
- Getahun Mekuria, Former Minster, Ministry of Innovation and Technology, Address on his tweet about the Telecom Privatization, /2020.
- Prime Minister Dr. Abiy Ahmed, Address on his conference with political parties on the Liberalization of Telecom Sector, /2020
- Prime Minister Dr. Abiy Ahmed, Address on his Conference with the task Force taking the responsibility to hold the privatization process, /2020.

5. Books

- John W. Creswell, Research Design, Qualitative, Quantitative and Mixed Approaches, (4th ed. 2014)

6. Journals and Articles

- "Article 19", Ethiopia: Proclamation on Telecom Fraud Offences, Legal Analysis, August 2012.
- "They Know Everything We Do", Telecom and Internet Surveillance in Ethiopia, Human Rights Watch, 2014.
- Arif Bramantoro, Information System Department, College of Computer and Information Sciences, Al-Imam Muhammad ibn Saud Islamic University, Riyadh, Saudi Arabia, Yousef Alraouji, Information System Department, College of Computer and Information Sciences, Al-Imam Muhammad ibn Saud Islamic University Riyadh, Saudi Arabia, International Call Fraud Detection Systems and Techniques, Conference Paper, September 2014, Research Gate, available at: https://www.researchgate.net/publication/275885973.
- Bypass Fraud, Interconnect and GSM Gateway Fraud, Executive Summary, Interconnect Bypass Detector,
- Cyber – Telecom, Crime Report 2019, Trend Micro Research, Europol's European Cybercrime Centre (EC3).

- Godfred Yaw Koi-Akrofi, Joyce Koi-Akrofi, Daniel Adjei Odai, and Eric Okyere Twum, Global Telecommunications Fraud Trend Analysis, ISSR Journals, SSN: 2028-9324, Vol. 25 No. 3, Feb. 2019.
- Halefom Hailu, "The State of Cybercrime Governance in Ethiopia", (2015).
- Huang Zuhe, Causes and Prevention of Telecommunication Network Fraud, Post-Doctoral Research Center of CCISR, Haidian District, Beijing China, ICHSSD, 2017.
- International Interconnection forum for Services over IP (i3 Forum), April 2012, www.i3Forum.org.
- Knife Micael Yilma and Halefom Hailu, The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E- Commerce and the New Media, Article in Mizan Law Review, October 2015.
- Kinfe Micheal Yilma, "Developments in Cybercrime Law and Practice in Ethiopia," *Journal of Computer Law & Security Review* (2014)
- Richard A. Becker, Chris Volinsky, and Allan R. Wilks, Fraud Detection in Telecommunications: History and Lessons Learned, Article in Technometrics, February 2010
- Telecoms and Media, an Overview of Regulation in 48 Jurisdictions Worldwide, Al Kamel Law Office, Egypt, 2011.

7. Other Documents

- A Report found from Information Network Security Agency, November 2017.
- A Survey Conducted by the Federal General Attorney, Challenges of the Implementation and Gaps of the Telecom Fraud Proclamation, unofficial, 2018.
- A Survey prepared by Information Network Agency on the legal Gaps of telecom Fraud Proclamation, unofficial, February 2016.
- Cyber Security Practices and Challenges at Selected Critical Infrastructure in Ethiopia: Towards Tailoring Cyber Security Framework.
- ICT Regulation Toolkit, Legal and Institutional Framework, ITU, infoDev, May 2016.
- International Telecommunications Union, World Conference on International Telecommunication, Final Acts, Dubai, 2012.

- Presentation, Marcel Belingue, Manager, Communications, CTO, An Overview of VoIP Regulation in Africa, Workshop on VoIP, Fourth Africa Internet Summit and Exhibition (AFRINET), Abuja, 23 January 2005.
- Telecoms: Ghana seizes 300,000 sim boxes from syndicates, by Dasmani Larii, posted on Friday, 8 April 2016 10:54, last accessed 11/2/2020, 11:55PM.
- Tewodros Getaneh, "Cyber Security Practices and Challenges at Selected Critical Infrastructure in Ethiopia: Towards Tailoring Cyber Security Framework", LLM Thesis, Addis Ababa University School of Law and Governance Studies, 2018.