ADDIS ABABA UNIVERSITY

COLLEGE OF LAW AND GOVERNANCE STUDIES, SCHOOL OF LAW

THE USE OF SPECIAL INVESTIGATION TECHNIQUES IN COUNTER-TERRORISM PROSECUTIONS IN ETHIOPIA: AN APPRAISAL OF THE LAW AND THE PRACTICE

By

BEBIZUH MULUGETA MENKIR

Supervisor

DR. WONDWOSSEN DEMISSIE (Associate Prof.)

MAY /2024

ADDIS ABABA, ETHIOPIA

THE USE OF SPECIAL INVESTIGATION TECHNIQUES IN COUNTER-TERRORISM PROSECUTIONS IN ETHIOPIA: AN APPRAISAL OF THE LAW AND THE PRACTICE

Thesis

Submitted in Partial Fulfillment of the Requirements for Master of Laws (LL.M) Degree in Criminal Justice

By

BEBIZUH MULUGETA MENKIR (GSR/3049/14)

Supervisor

DR. WONDWOSSEN DEMISSIE (Associate Prof.)

May /2024

ADDIS ABABA, ETHIOPIA

DECLARATION OF ORIGINALITY

I affirm that this thesis titled "*The Use of Special Investigation Techniques in Counter-Terrorism Prosecutions in Ethiopia: An Appraisal of the Law and the Practice*" is my own original work and has not been previously submitted to Addis Ababa University or any other educational institution. To the best of my knowledge, it has not been published before and I have also appropriately acknowledged all the sources that are used in this study.

Bebizuh Mulugeta Menkir (GSR 3049/14)

Signature……

May/ 2024

Thesis Approval Page

This LLM thesis written by Bebizuh Mulugeta Menkir titled "*The Use of Special Investigation Techniques in Counter-Terrorism Prosecutions in Ethiopia: An Appraisal of the Law and the Practice*" has been approved by the following members of the examining board.

Examining Board Members

Thesis Supervisor - Dr. Wondwossen Demissie

Signature.....

May/ 2024

Examiner 1 - Dr. Simeneh Kiros

Signature.....

May/2024

Examiner 2 - Ato Worku Yaze

Signature.....

May/2024

Table of Contents

DEDICATION

In loving memory of my dear, dedicated and caring father **Mulugeta Menkir Temesgen (** *Babeche*).

Dear *Babeche;*

You were my pride and a person that I was always looking up to. I am not lucky enough to have you with me anymore and I feel like I have lost my compass, because your untimely and unexpected departure left me in the middle of nowhere.

Babeche, there are certain things in life that we tend to deny; no matter how we know that they are true. The late *Sibhat G/Egeziabeher* once described the idea of death as 'false, until it is real'. And it is when I missed you that I have come to really understand what he meant by that. I know that man is mortal and all of us are on a queue to death. However, I didn't see this in your case, up until I encountered with the hard moment of truth on that unfaithful day. Till that day, I was totally forgetful of death and naively imagining you being an octogenarian, nonagenarian or even more. To my dismay and severe regret that was not meant to happen.

Babeche, it is still difficult for me to accept your passing. I don't also think that I can reconcile with this fact any time soon. Since you have gone, there are only few days (if any) that have passed without seeing you in my dreams. I cannot forget the discussions that we had on a host of issues; together with your sharp critiques as well as playful remarks on my rather not well thought ideas (attitudes). I cannot also forget your phone calls to me every day at 9:00 P.M. This is not to mention the great value that you had towards education, your love for books and reading, which will remain with me forever. What can I say, with all these and many others, you will continue to have a towering presence in my life.

I am really missing you and will continue to miss you so much. May your soul rest in eternal peace, *Babecheye*!

ACKNOWLEDGEMENT

First and foremost, I would like to extend my sincere gratitude to my thesis supervisor Dr. *Wondwossen Demissie* for his invaluable advice and encouragement, by responding to my recurrent emails, even before I officially started to write this thesis. Indeed, this thesis would not have gotten its present shape in the absence of his invaluable comments. Working under his supervision has been an enriching academic experience for me that I am very much thankful for.

Next, I would like to thank my father, *Mulugeta Menkir (Babeche*), and my mother, *Banchigize Leyew (Tatey*), for their continuous encouragement in the course of my study. My father's reminder every time he thought that I was not proceeding well in writing my thesis means a lot to me. Most importantly, I am very much indebted and thankful to *Fedila Shehebo (Fiyuu)* for staying beside me, in times of my difficulty, and offering her immeasurable care and support in literally everything that I want for the completion of my study and this thesis. I am also grateful to my siblings *Senaite Mulugeta cum Yihenew Wubet* , *Heruye Mulugeta* and *Maheder Mulugeta* for their moral support during my study.

My thank should also extend to my good friends *Robel Kidane, Habtamu Zewdu, Dr. Yonas Girma, Zemenu Tarekegn, Belete Addis, Shimelash Wondale* and *Anteneh Ayalew* for helping me in the different stages of writing this research.

The last but not the least, I should also thank the Judges, Prosecutors, Investigative Police Officer and others who were willing to respond to my interviews. It is equally appropriate to thank the officers in Federal High Court Registrar and Ministry of Justice dead file depositories who helped me in getting the files that I want for my research.

And finally, as Nelson Mandela once said "it always seems impossible until it is done".

ACRONYMS

ACHPR	African Charter on Human and Peoples Rights
ATP	Anti-Terrorism Proclamation (Procl. No 652/ 2009)
AU	African Union
CPC	Criminal Procedure Code of Ethiopia
FDRE	Federal Democratic Republic of Ethiopia
ICCPR	International Covenant on Civil and Political Rights
NISS	National Intelligence and Security Service
OAU	Organization of African Union
PSTCP	The Prevention and Suppression of Terrorism Crimes Proclamation (Procl. No 1176/2020
SITs	Special Investigation Technique(s)
UDHR	Universal Declaration of Human Rights
UNCTOC	United Nations Convention on Transnational Organized Crime
UNODC	United Nations Office on Drugs and Crimes
UN	United Nations
UNSC	United Nations Security Council
UNGA	United Nations General Assembly

ABSTRACT

Criminal justice measures to counter-terrorism shall be proactive so as to reduce the occurrence of terrorist attacks. This approach, among others, involves using SITs which are secretive methods that can be used to gather information/evidence without alerting the suspect. Though SITs are helpful for the prevention and investigation of terrorism, there are also human rights concerns raised in the use of SITs. This makes it necessary to balance human rights and security by setting preconditions of the use of SITs. Under the PSTCP Police can employ SITs subject to the preconditions that shall be fulfilled to use them for counter-terrorism investigations. In addition, NISS is responsible to follow up terrorism according to its establishment proclamation.

This research examines the law and the practice in use of SITs in counter-terrorism in Ethiopia. By employing qualitative and quantitative research methodologies, this research finds out that Ethiopian federal police is not using SITs that the anti-terrorism prosecutions are dependent on technical investigation reports prepared by NISS. Even if court authorization is a precondition to use SITs, none of the court cases and investigation files studied in this research contains evidence of court authorization. And it can be presumed that the evidences were gathered without court warrant. There are divergent practices, in court as well as prosecutorial decisions, in scrutinizing the legality of evidences obtained through SITs. In addition, despite the fact that PSTCP obliges for evidences gathered through SITs to be presented in the same way as they are obtained, in the actual practice prosecutions are being conducted by using technical investigation reports as evidence. As the judgments in the court cases, the evidences could not be presented directly because they are classified as 'top-secret'. The courts as well as prosecutorial decisions show inconsistency in scrutinizing the legality of the evidences and admitting/using technical investigation reports as evidence as well.

For better implementation of the law on SITs this research recommends, among others, the Ethiopia Federal Police shall start using SITs by its own. In addition, a detailed legal framework on intelligence/evidence exchange between NISS and other law enforcement organs shall be enacted.

Key terms:- Counter-terrorism, Ethiopia, Special Investigation Techniques (SITs), Prosecutions

CHAPTER ONE

1. INTRODUCTION

1.1 Background of the Study

An increasing threat that terrorist acts have posed to societal peace and security pushed states to design criminal justice responses to counter terrorism.[1] In this regard, the UN General Assembly and Security Council resolutions require states to take steps to counter terrorism by, among others, enacting counter-terrorism legislations criminalizing the commission, preparation and planning of terrorist acts.[2] In addition, even if there is no a comprehensive international convention on terrorism, different international conventions oblige states to criminalize hijacking, hostage taking, offence against maritime security, financing of terrorism and other specific conducts that are related to terrorism.[3] In the African context, the 'OAU Convention on the Prevention and Combating of Terrorism' obliges state parties to criminalize terrorist acts in their respective national legal frameworks.[4]

In addition to criminalizing acts of terrorism, states have also adopted a proactive approach to counter terrorism, also referred to as precautionary approach, which aims at preventing terrorist attacks.[5] This proactive approach to counter terrorism allows '…..intervention against terrorism

[1] United Nations Office on Drugs and Crime(UNODC), *Handbook on Criminal Justice Responses to Terrorism*, Criminal Justice Handbook Series (2009) 5< https://www.unodc.org/documents/terrorism/Handbook_on_Criminal_Justice_Responses_to_Terrorism_en.pdf > accessed 3 May 2023

[2] UN General Assembly, A/RES/60/288 on The United Nations Global Counter-Terrorism Strategy,[Sept 2006] < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement > accessed 18 May 2023 UN Security Council, S/RES/1373 [Sept 2001] < https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf > accessed 18 May 2023.

[3] Chirstiane Bourloyannis-Vrailas, *United Nations Human Rights Standards as Framework Conditions for Anti-Terrorist Measures: Anti-Terrorism Measures and Human Rights*, (Wolfgang Bendek and Alice Yotopoulos-Marangopoulos eds, Maritinus Nijhoff Publishers 2004) 13&14.

[4] OAU Convention on the Prevention and Combating of Terrorism, [14 June 1999], Art 2,< https://au.int/sites/default/files/treaties/37289-treaty-0020_-oau_convention_on_the_prevention_and_combating_of_terrorism_e.pdf> accessed 3 May 2023.

[5] Wondwossen Demissie, 'How to Rescue Human Rights from Proactive Counter Terrorism in Ethiopia' (2017) XXIX Journal of Ethiopian Law 25, 27&29; UNODC Handbook on Criminal Justice (n 1).

planning and preparation before they mature in to action'[6] This approach conventionally involves what are referred to as 'special investigation techniques (SITs)'.[7]

Moreover, subject to the basic principles and conditions of domestic laws, 'UN Convention on Transnational Organized Crime (UNCTOC)' has recognized (SITs) as effective ways to tackle organized crimes.[8]

There is neither a universally accepted legal definition nor exhaustive list for what constitute SITs, [9] the Council of Europe recommendations defined SITs as follows.

> ….techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons.[10]

In counter terrorism, the use of SITs is justified because the sophistication and secretive nature of terrorist networks makes it difficult to tackle these types of crimes through traditional crime investigations techniques.[11] Due to their potential to cause large scale destructions, the law enforcement organs shall also strive to prevent the commission of terrorist acts by thwarting

---

[6] Wondwossen, ibid 28 citing United Nations Office on Drugs and Crime Terrorism Prevention Branch, *Preventing terrorist acts: A Criminal Justice Strategy Integrating Rule of Law Standards in Implementation of United Nations Anti-Terrorism Instruments* (2006) < https://www.unodc.org/pdf/terrorism/TATs/en/3IRoLen.pdf> accessed 24 Oct 2023.

[7] UNODC < https://www.unodc.org/unodc/en/terrorism/latest-news/2022_unodc-supports-mali-on-the-use-of-special-investigative-techniques-in-terrorism-investigations.html > accessed 3 May 2023. For what constitutes 'special investigation techniques' see Chapter 2.1 below.

[8] UN Convention on Transnational Organized Crime (UNCTOC) [Sept 2000] Art 20 < https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf > accessed 26 Oct 2023.

[9] United Nations Office on Drugs and Crime(UNODC), *University Module Series on Counter-terrorism, Module 12: Privacy, Investigative Techniques and Intelligence Gathering,* (July 2018) < - https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/special-investigative-techniques.html > ; accessed 29 Sept 2023 ; Worku Yaze, 'The Use of 'Special Investigation Techniques and Tools' in the Fight against Serious Crimes: Legal Basis and Human Rights Concerns in Ethiopia' (2018) XXX Journal of Ethiopian Law 81, 85.

[10] Council of Europe Committee of Minsters Recommendations Rec(2005)10 on "Special Investigation Techniques" in relation to Serious Crimes including Acts of Terrorism, (April 2005) < https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Rec_2005_10.pdf > 26 Oct 2023.

[11] Worku (n 9) 82, 84 & 91.

terrorism plots.[12] This makes it necessary to employ SITs that would enable the law enforcement organs to gather information which will be useful to gather information about terrorist plots ahead of time and foil them before they are actually committed.[13]

In addition, such techniques are important to gather evidence that can be presented as evidence in future prosecutions against the suspects.[14] As traditional investigation techniques can hardly accomplish all these functions, 'the use of SITs and tools is really borne of necessities.'[15]

Nevertheless, intrusive nature of proactive approach to counterterrorism in general and SITs in particular makes them susceptible to be abused or misused potentially resulting in adverse impact on human rights.[16] In non-democratic societies SITs be used by the government against political opponents.[17] And at times, in anti-terrorism prosecutions involving SITs, law enforcement agencies may want to keep the secrecy of the source and methods used to gather evidence; which in turn raises questions on the fairness of the trial.[18] Evidence extracted through SITs may also be altered or misconstrued in a way that raises concerns on their reliability.[19]

As counter-terrorism measures shall be consistent with human right norms, principles and standards,[20] the use of SITs shall be regulated by law that balances human rights and counter-terrorism efforts.[21]

In the Ethiopian context, the "Anti-terrorism Proclamation"[22] (ATP) was the first special counter-terrorism legislation. Among others, the ATP incorporated provisions concerning SITs

---

[12] ibid 92.
[13] ibid 83&87.
[14] ibid 83&87.
[15] ibid 84.
[16] Quirine Eijkman, and Daan Weggemans, 'Visual Surveillance and the Prevention of Terrorism: What about the Checks and Balances?'(2011) 25(3) International Review of Law, Computers & Technology143, 143; Quirine Eijkman, 'Preventive Counter-terrorism and Non-discrimination Assessment in the European Union' (2011) 2 Security and Human Rights 90.
[17] ibid.
[18] UNODC University Module (n 9).
[19] Gabriella Di Paolo, 'Judicial Investigations and Gathering of Evidence in a Digital Online Context' (2009) 80 International Review of Penal Law 201, 202 < https://www.cairn.info/revue-internationale-de-droit-penal-2009-1-page-201.htm> accessed 27 Oct 2023.
[20] Salma Yusuf, 'The Resilience of the Human Rights Norm in an Era of Counter-Terrorism' (2012) 28 UNISCI Discussion Papers 183, 190 < https://www.ucm.es/data/cont/media/www/pag-72494/UNISCI%20DP%2028%20-%20YUSUF.pdf > accessed 27 Oct 2023; UNODC Handbook on Criminal Justice (n 1).
[21] UNODC University Module (n 9); Worku (n 9) 84&94.

to counter terrorism. In this respect, National Intelligence and Security Service (NISS) was authorized to intercept and conduct surveillance on individual communications with court warrant.[23] Intelligence reports that do not disclose the source and method of information gathering were also admissible items of evidence in anti-terrorism prosecutions.[24]

The contents and application of the ATP had been criticized for adversely affecting human rights and rule of law in Ethiopia.[25] In the year 2020, the ATP was replaced by a new proclamation namely; "Prevention and Suppression of Terrorism Crimes Proclamation"[26] (here after referred as the PSTCP).

Among others, the PSTCP aims to mend the adverse impacts that the ATP had caused on fundamental human rights.[27] The use of SITs in counter- terrorism is one of the areas of improvement in the PSTCP. And this research aims to examine the law and the practice in the use of SITs to counter terrorism, as evidenced from the court cases and anti-terrorism criminal investigation files.

1.2 Statement of the Problem

Despite their benefits, SITs have also the potential to be misused or abused in a way that adversely affect fundamental human rights , rule of law and public trust in the criminal justice administration.[28]

As human rights and counter-terrorism shall not be mutually exclusive,[29] SITs to counter terrorism shall be utilized in a way that give due regard to human rights and rule of law. States

---

[22] Anti-terrorism Proclamation, Proclamation No. 652/2009, (Fed. *Negarit* Gazette, 15th Year No. 57).

[23] ibid, Art 14.

[24] ibid, Art 23.

[25] See for instance, Zelealm Kibret, 'The Terrorism of 'Counterterrorism: The Use and Abuse of Anti-Terrorism Law, the Case of Ethiopia (2017) 13(13) European Scientific Journal 505, 516&517; **የሽብር ወንጀልን ለመከላከል እና ለመቆጣጠር በተዘጋጀ ረቂቅ አዋጅ ላይ የተዘጋጀ አጭር ማብራሪያ** (**የሽብር ወንጀልን ለመከላከል እና ለመቆጣጠር በተዘጋጀ ረቂቅ አዋጅ የዝግጅት ሰነድ፣ በኢፌድሪ ጠቅላይ አቃቤ ሕግ፣ የሕግና ፍትሕ ገዳዮች አማካሪ ጉባኤ፣ 2012 ዓ.ም**) 216; Amerti Solomon, 'Appraising the Reform of the Anti-Terrorism Proclamation of Ethiopia Based on Applicable Human Rights Standards',(2020) , XII Ethiopian Human Rights Law Series, 125, 128.

[26] Prevention and Suppression of Terrorism Crimes Proclamation (PSTCP), Proclamation No 1176/2020 (Fed *Negarit* Gazette, 26th Year No. 20).

[27] PSTCP, ibid., Preamble , para. 4; **የአዋጅ አጭር ማብራሪያ**(n 25).

[28] Eijkman and Weggemans,(n 16) 143. Worku (n 9) , 84&94.

are duty bound to ensure that SITs are not violating of human rights. To this end, the use of SITs shall be regulated by legal frameworks that strike a proper balance between human rights and security.[30] In this respect, SITs shall be used only to the extent they are necessary and proportionate to achieve their legitimate objective of combating terrorism.[31] Determining the appropriateness or otherwise of using SITs in a given case shall be made an impartial organ other than the one implementing them.[32] There shall also be proper accountability mechanisms in case when there is an abusive utilization of SITs by governmental law enforcement and security organs.[33]

While the ATP was in force, Ethiopian courts were criticized for failing to properly safeguard human rights in anti-terrorism prosecutions, including those using evidences that were alleged to have been obtained through illegal utilization of SITs.[34]

As noted, PSTCP is enacted with the objective of maintaining human rights and rule of law in the course of combating terrorism in Ethiopia, including in the use of SITs. However, the existence of the law doesn't necessary mean compatibility between the law and the practice.[35] As this may also be true in the case of the PSTCP, which has come to force more than three years ago[36], it would not be too early to examine the law and the practice in the use of SITs in counter-terrorism in Ethiopia.

---

[29] Yusuf (n 20)186 .

[30] UNODC, University Module (n 9); Worku (n 9) 84& 94.

[31] The Thirteen International Principles on the Application of Human Rights to Communication Surveillance, < https://www.eff.org/files/necessaryandproportionatefinal.pdf> accessed 9 Feb 2023.

[32] UNODC Hand Book (n 1), 54; UNODC, *The Current Practice in Electronic Surveillance in the Investigation of Serious Organized Crimes*, (United Nations Publications 2009) 15 < https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf > accessed 28 Oct 2023.

[33] ibid.

[34] See for instance, Wondwossen Demessie, 'Court's Reluctance to Safeguard Rights of Accused in the Ethiopian Counter-terrorism Prosecutions and its Broader Implications'(2022) 16(1) Mizan Law Review 193, 200-203; Hiruy Wubie Gebreegziabher, 'The Right to Privacy in the Age of Surveillance to Counter terrorism in Ethiopia' (2018) 18 African Human Rights Law Journal 392, 398.

[35] Helen Duffy, 'Global Trends in Counter-terrorism Implications for Human Rights in Africa', (Institute for Security Studies, Monograph 206 2023) 36 < https://issafrica.s3.amazonaws.com/site/uploads/mono-206.pdf> accessed 28 Oct 2023.

[36] The PSTCP entered in to force on 25th of March, 2020.

1.3 Objectives of the study

General Objective.

The general objective of this research is to examine the law and the practice in use of SITs in counter-terrorism in Ethiopia.

Specific Objectives

This research specifically aims to:

- Examine the human rights concerns in the use of SITs to counter terrorism.
- Identify and analyze the preconditions to using SITs in counter terrorism investigations in Ethiopia.
- Assess the prevalence in the use of SITs in counter-terrorism investigation in Ethiopia and the practice in obtaining court authorization.
- Examine the effects of non-compliance with the law on the status of the evidence obtained through SITs.

1.4 Research Questions

This research will answer the following research questions.

1. What are the human right concerns in the implementation of SITs to counter terrorism?
2. What are the preconditions for employing SITs in counter terrorism investigations?
3. How often terrorism investigations in Ethiopia involve SITs and in what proportion of these instances the law enforcement obtained prior court authorization?
4. What is the effect of non-compliance with the law on the status of the evidence obtained through special investigation techniques?
5. What are the salient problems observed in the application of the law on SITs in counter terrorism in Ethiopia?

1.5 Research Methodology

The research is a mixed research type employing qualitative and quantitative research methodology. As such, while the research questions 1, 2, 4 and 5 above have doctrinal and qualitative features. The research question 3 will be dominantly quantitative informed by data from the Federal High Court, the Ministry of justice, the Federal Police Commission, the Ethiopian Telecom.

1.5.1 Data Sources and Method of Data Collection

The research uses primary and secondary data sources. In this regard, national and international laws, federal court cases, criminal investigation files will be the primary data sources. In addition, books, scholarly articles and reports of governmental and non-governmental organ are also used as secondary data sources.

When it comes to method of data collection, review of federal anti-terrorism court cases and anti-terrorism criminal investigation files was employed. In addition, interviews were also conducted with federal court judges, prosecutors, investigative police officers and *Ethio-telecom* officials.

1.5.2 Population Size and Sample Size Determination

For the research questions that require empirical data, cases over which special investigations techniques have been employed have been identified from the total anti-terrorism court cases and investigation files in the Federal High Court and Ministry of Justice respectively. As noted, the focus of this research is on cases that are entertained after the coming in to force of PSTCP.

From March 2020 to June 2023, the total numbers of anti-terrorism cases decided by the Federal High Court are 52.[37] In addition, from March 2020 to May 2023 there are 59 criminal investigation files on terrorism that the federal prosecutor decided not to prosecute for lack of sufficient evidence as per Art 42(1)(a) of the Criminal Procedure Code of Ethiopia.[38] For the purpose of this research, investigations conducted through SITs are identified from these two groups of files.

[37] Federal High Court (*Lideta* Branch) database, accessed June/2023. The 52 cases decided do not include cases that had been started before the PSTCP come to force.
[38] The Ministry of Justice (Transnational and Organized Crimes Directorate) database, accessed May/2023.

Though the original plan was to examine all of the above mentioned cases, time constraint and the unavailability of files in the Federal High Court and Ministry of Justice depositories has made it necessary to limit the number of cases reviewed based on data (file) availability. Accordingly, a total of 35(out of 52) court cases and 44 (out of 59) anti-terrorism investigation files have been reviewed with a view to get information if SITs were used.

In this way, since only 12 court cases and 10 criminal investigation files found are related to SITs and used in this research for further analysis. Thus, a total of 22 real cases have been used to write this research.

In addition, interview is conducted with two federal court judges, one federal prosecutor, one federal investigative police officer and one *Ethio-telecom* official.

1.6 Limitation of the study

Shortage of time and unavailability of the court and criminal investigation files in the dead file depositories of the court and Ministry of Justice were the major problems faced in the course of conducting this research work.

Moreover, as observed from real cases the subject matter of this research is also related to classified information, which makes it difficult to get primary data from NISS.

1.7 Scope of the Study

The focus of this research is on the anti-terrorism prosecutions conduced after the PSTCP has come to force. And hence, anti-terrorism prosecutions that were entertained as per the ATP are not within the scope of this research. Few court cases that were started under the ATP; but later on requested to be entertained by the PSTCP are covered in the qualitative parts of this research. In addition, as the focus of the research is on counter-terrorism prosecutions in the High Court cases, the decisions that the Federal Supreme Court of Ethiopia might have given, over the cases, in its appellate jurisdiction has not covered in this research.

1.8 Significance of the Study

While there is lack of academic research conducted on the area, the paper written by Wondwossen Demissie pinpoints the problems as well as the commendable aspects in the

decisions rendered by the Federal High Court of Ethiopia; in safeguarding the rights of the accused individuals in anti-terrorism prosecutions.[39] This paper also recommends for further studies to be conducted in the area.

As such, this research contributes by offering an evidence based finding on the law and practice in the use of SITs in counter terrorism prosecutions in Ethiopia. In this regard, this research identifies the problems and how the court and the office of the Prosecutor are handling cases involving evidence obtained through SITs. This research also recommends measures so as to improve the implementation of the law on SITs in a way that safeguards the rights of the accused.

[39] Wondwossen Demessie, 'Court's Reluctance to Safeguard Rights of Accused in the Ethiopian Counter-terrorism Prosecutions and its Broader Implications' (2022) 16(1) Mizan Law Review, 193-208.

CHAPTER TWO

2 SITs IN COUNTER-TERRORISM AND HUMAN RIGHTS CONCERNS

2.1 The Meaning and Significance of SITs in Counter-terrorism

There is no single and universally agreeable definition for 'SITs.'[40] In this regard, there are two approaches of defining what constitutes SITs. The first approach is a functional definition by listing some techniques which can be considered as SITs.[41] For instance, the UNCTOC rather than providing a comprehensive definition for SITs, recognizes them by mentioning some techniques that can be considered as such.

> If permitted by the basic principles of its domestic legal system, each State Party shall, within its possibilities and under the conditions prescribed by its domestic law, take the necessary measures to allow for the appropriate use of ……. **special investigative techniques, such as electronic or other forms of surveillance and undercover operations,** by its competent authorities in its territory for the purpose of effectively combating organized crime.[42] (emphasis mine)

On the other hand, there is a comprehensive definition for SITs provided by 'Council of Europe Committee of Minsters Recommendation' which reads as;

> SITs…techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons.[43]

---

[40] UNODC University Module Series (n 9).

[41] Hans G. Nilsson, 'Special Investigation Techniques and Developments In Mutual Legal Assistance - The Crossroads Between Police Cooperation and Judicial Cooperation', 125th International Training Course Visiting Experts' Papers, 65 Resource Material Series,, 39, 40 , available at: <https://www.unafei.or.jp/publications/pdf/RS_No65/No65_07VE_Nilsson2.pdf,> accessed on 24/10/2023

[42] United Nations Convention against Transnational Organized Crime, Art 20(1).

[43] 'Council of Europe Committee of Minsters Recommendations' "Special Investigation Techniques" in relation to Serious Crimes including acts of Terrorism, Rec(2005) 10, Adopted by the Committee of Ministers on 20 April 2005 at the 924th meeting of the Ministers' Deputies, Chapter I.

According to the comprehensive definition stated above, the SITs are characterized by their secretive way of gathering evidence or intelligence about a certain criminal plot and their application could interfere with basic human rights.[44]

SITs have a pivotal role in counter terrorism,[45] because detection and prevention of terrorist attacks is difficult owing to the secrecy and complexity of terrorism/ terrorist networks and the changing methods used to perpetrate terrorist acts.[46] Moreover, unlike ordinary crimes physical evidences and/or externally observable behaviors may not necessarily exist in organized crimes like terrorism.[47] The perpetrators may not also be physically present at the place of commission of the crime or the crime scene and leave no traces on the crime.[48] These unique features will make it difficult to tackle terrorism with the commonly available legal regimes for criminal justice, human rights and rules of law.[49]

Furthermore, if they are actually committed, terrorism acts will cause serious impacts on peoples' life, property and overall wellbeing of the society; prevention is much more preferable to prosecution.[50] And hence, the criminal justice response to counter-terrorism shall primarily focus on preventing these crimes from being committed.[51]

Preventing the commission of a terrorist acts through ordinary criminal justice measures is hardly possible; because ordinary criminal justice responses are more of reactive responses coming after the commission of a crime.[52] Even after the commission of the crime, witnesses may not cooperate with law enforcement organs fearing the potential reprisals coming from terrorist networks.[53] This makes it important to design a proactive criminal justice response to

[44] ibid, preamble, para.14 &16.
[45] ibid, preamble, para.15.
[46] UNODC Handbook on Criminal Justice (n 1) 5, 49-50; Worku (n 9) 91.
[47] Worku (n 9) 91&92.
[48] Alessandro Lentini, 'Selected Issues in Counter-terrorism: Special Investigative Techniques and the International Judicial Cooperation Focus on the European Union', (2019) 4 < https://www.dirittopenaleglobalizzazione.it/wp-content/uploads/2018/03/Alessandro-Lentini-Selected-Issues-in-Counter-Terrorism.pdf > accessed 1 Nov 2023; Worku (n 9) 91 and 92.
[49] UNODC Handbook on Criminal Justice (n 1) 5& 49.
[50] Worku (n 9) 91; Wondwossen (n 5) 29.
[51] Worku (n 9) 91; Wondwossen (n 5) 29.
[52] UNODC Handbook on Criminal Justice (n 1) 5; Worku (n 9) 91 &92.
[53] Worku (n 9) 92.

counter terrorism which aims at preventing terrorist attacks, among others, by employing effective investigation powers and techniques.[54]

The use of SITs play instrumental role in obtaining intelligence and information regarding the operation of clandestine terrorist networks and foil terrorist plots before they are actually committed.[55] As these are valuable information that would otherwise be difficult to get through other means,[56] "the use of SITs and tools is really borne of necessities"[57]

At times, ordinary criminal punishment is unable to deter the commission of crimes of terrorism because of the presence of terrorists who are committed to die for their cause.[58] In such type of cases, uncertainty on the probability of being apprehended before the commission of the terrorist acts serves the deterrence purpose better than the punishment.[59] As SITs are employed secretly, it can be argued that the potential terrorists would be fearful of and cannot be certain as to the probability of being under police or security agencies surveillance and follow up. In effect, these fears of uncertainty will deter the potential terrorists from taking practical steps to commit terrorist acts.

2.2 Types of SITs to Counter Terrorism

The SITs to counter-terrorism are "numerous, varied and constantly evolving"[60] that an exhaustive list of such techniques hardly exist.[61] Indeed, rather than providing an exhaustive list, laws shall be flexible so as to accommodate technological advancement and newly emerging special investigation techniques.[62]

---

[54] UNODC Handbook on Criminal Justice (n 1) 3,5&49. A proactive counter-terrorism response includes " a comprehensive system of substantive offences, investigative powers and techniques, evidentiary rules and international cooperation." (UNODC Handbook on Criminal Justice (n 1) 5.
[55] ibid 54.
[56] UNODC, 'Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crimes' (2009)1 < https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf> accessed 26 Oct 2023 ; Worku (n 9) 93-94.
[57] Worku (n 9) 84.
[58] Wondwossen (n 5) 30.
[59] ibid 30.
[60] Council of Europe Recommendations (n 43) preamble para.13.
[61] UNODC University Module Series (n 9) .
[62] Lentini (n 48) 4&5.

That said there are SITs that are commonly used in counter terrorism which includes surveillance, interception of communication, wire-tapping, eavesdropping infiltration, simulated relationships.[63] In the Ethiopia case, the PSTCP recognizes surveillance, interception, infiltration and creating simulated communication.[64]

Though an in-depth examination on the types of SITs in counterterrorism is not the objective of this research, the basic characteristic features of the commonly used techniques is presented as follows.

Surveillance, within the context counter-terrorism, can be defined as "the collection or monitoring of information about an individual/individuals through the use of technology."[65] And it encompasses visual surveillance, audio surveillance, data surveillance, tracking surveillance. Surveillance involves, among others, the covert use of video camera, audio recorder/eavesdropping, wiretapping, intercepting electronic communications, tacking movements through Global Positioning Systems (GPS) and others.[66]

Interception of communication is a very useful and effective form of surveillance mainly because terrorist acts are undertaken by means of communication; including online communications.[67] As there is no international legal framework on what constitutes interception,[68] the task of defining interception is left for domestic laws.[69] Interception of communication can be implemented in different ways including phone tapping and by installing malwares on cellphones and personal computers.[70]

---

[63] UNODC University Module Series (n 9) .
[64] PSTCP (n 26) Art. 42 (1)(a-d).
[65] UNODC Current Practice in Electronic Surveillance (n 56) 4-5.
[66] ibid,2,4-5;Worku (n 9) 87&88; Council of Europe, *The Deployment of Special Investigative Means*, Criminal Asset Recovery Project in Serbia, (2013)12 < https://rm.coe.int/deployment-of-special-investigative-means-eng/16807828fa > accessed 26 Oct 2023.
[67] Lentini (n 48) 4&5. In some countries , interception of communication and surveillance are considered as the same; while others draw a distinction between the two ;because interception is more intrusive than surveillance ; which necessitates to regulate each under a separate legal frameworks. (see Council of Europe, (n 66), 60-61).
[68] Lentini (n 48) 6.
[69] ibid, 4. In Ethiopia, the PSTCP does not also provide a definition for interception. But in the context of computer crimes, interception is defined as; "real-time surveillance, recording, listening, acquisition, viewing, controlling or any other similar act of data processing service or computer data." (Computer Crimes Proclamation, Proclamation No. 958/2016, 22nd Year, No. 83, Art 2(13)).
[70] ibid, 4&5.

Infiltration is the other SITs that involves the use of undercover officers or undercover criminal informants who would directly engage with the suspects and follow up the criminal plot.[71] In infiltration, the operation can be conducted through physical engagement with the suspects or virtually, by using internet and social media platforms.[72]

In infiltration, the degree of deception differs depending on the role that the undercover operators play with the suspects. The undercover operator may deliver false information, collaborate and/or entice the suspects to commit the crime.[73] And in other cases, the undercover agent may have a limited role of letting the suspects pursue their plan and catch them on the spot.[74]

2.3 The Relationship between SITs and Human Rights in Counter-terrorism

It is generally agreed that there is a direct and indirect relationship between counter terrorism and human rights.[75] Terrorism is a serious violation of human rights causing multiple causalities on the life, bodily integrity and property of numerous individuals.[76] Counter-terrorism measures too, have the potential to violate human rights like freedom of movement, freedom of expression, freedom of religion, and right to privacy.[77] As a result, there is a need to draw a balance between security and human rights while countering terrorism.[78]

There are philosophical divides regarding the relationship between counterterrorism measures and human rights.[79] The first one is the 'realist perspective' that considers violation of

[71] ibid, 9; Worku (n 9) 88.
[72] Lentini (n 48) 9.
[73] Worku (n 9) 88-89.
[74] ibid 88-89.
[75] Yusuf (n 20) 186.
[76] See for instance, The United Nations Global Counter-Terrorism Strategy, Resolution adopted by the General Assembly on 8 September 2006, para 1 and Annex Plan of Action , Art I; OAU Convention on the Prevention and Combating of Terrorism, preamble (Para. 9); Stella Margariti, 'Defining International Terrorism to Protect Human Rights' (2018) 29 Security and Human Rights 173, 174; UNODC Handbook on Criminal Justice (n 1) 6.
[77] Ilya Sobol, Michael Moncrieff, and Gloria Gaggioli, 'Exploring Counterterrorism Effectiveness and Human Rights Law' (2023)Working Paper, Geneva Academy of International Humanitarian Law and Human 5-8< https://www.geneva-academy.ch/joomlatools-files/docman-files/Working%20Paper%20-%20Counterterrorism%20Effectiveness%20and%20Human%20Rights%20Law.pdf> accessed 25 Oct 2023.
[78] Emanuel Gross, 'The Struggle of a Democracy against Terrorism -Protection of Human Rights: The Right to Privacy versus the National Interest - the Proper Balance' (2004) 37(1) Cornell International Law Journal 28, 29.
[79] Eran Shor and Daniel Sailofsky, *Human Rights and Terrorism: Issues and Overview* (International Human Rights and Counter Terrorism, Eran Shor and Stephen Hoadley eds , 2019) 2; Salma Yusuf (n 20) 186; Gross (n 78) 29.

fundamental human rights as inevitable while taking preemptive measures to combat terrorism.[80] In the 'realist perspective', terrorists are presumed to have willfully forfeited their human rights protection that terrorist attacks shall be foiled by any means necessary; including by violating the human rights of terrorist.[81] Accordingly, this view is in favor of restricting human rights because more human rights would lead to more terrorist attacks. [82] As the threats and outcomes of terrorism compel states to resort to security measures at the expense of human rights, it is taken as willingness to be less free for the purpose of being safe.[83]

On the other hand, the 'civil libertarian perspective' argues in favor of '...the supremacy of international human rights over national security'.[84] This view stands against breaching fundamental human rights in the name of counterterrorism; because doing so 'undermines the moral authority of democracies, hurts international cooperation, and erodes public support.'[85]According to this perspective, depriving human rights in the name of security is '… to put oneself on the same moral plane as the terrorists, for whom the end justifies the means.'[86] In addition, violation of human rights in counter terrorism is taken as an indirect support for terrorism because 'terrorism often thrives when human rights are violated.'[87]

The third approach is what is referred to as 'the nuanced approach', which argues for maintaining the balance between security and human rights, with in the human rights system itself; so as to avoid trade-off between these values.[88]

---

[80] Shor and Sailofsky (n 79) 2 ; Alison Brysk, *Human Rights and National Insecurity , National insecurity and Human rights Democracies Debating Counterterrorism*, (Alison Brysk and Gershon Shafir eds. University of California Press 2007) 10.

[81] Shor and Sailofsky (n 79) 2.

[82] Axel Dreher, Martin Gassebner and Lars-H. Siemers, 'Does Terrorism Threaten Human Rights? Evidence from Panel Data' (2010) 53(1) The Journal of Law & Economics 65, 65-67.

[83] Gross (n 78) 30.

[84] Brysk (n 80)10.

[85] Shor and Sailofsky (n 79) 2.

[86] Christopher Michaelsen, 'Balancing Civil Liberties against National Security? A Critique Of Counterterrorism Rhetoric' (2006) 29(2)UNSW Law Journal (2006), 2, see also Jolyon Ford, 'African counter-terrorism legal frameworks a decade after 2001' (2011) Institute for Security Studies(ISS), Monograph 177, 1 < https://issafrica.s3.amazonaws.com/site/uploads/Mono177.pdf > accessed 27 Oct 2023.

[87] Digest of Jurisprudence of the UN and Regional Organizations on the Protection of Human Rights While Countering Terrorism, 9 < https://www.ohchr.org/sites/default/files/Documents/Publications/DigestJurisprudenceen.pdf > accessed 27 Oct 2023.

[88] Yusuf (n 20) 186; United Nations Office of the High Commissioner on Human Rights, United Nations Counter-Terrorism Implementation Task Force: CTITF Working Group on Protecting Human Rights while Countering

Be the philosophical debates as they are, states have the right and the responsibility to protect individuals from terrorist attacks.[89] Criminal justice responses are one of the measures that are used to protect human rights from terrorist attacks.[90] As such, individuals who have participated in terrorism or related acts shall be held criminally responsible for serious human right violations.[91]

As noted, criminal justice measures to counter-terrorism shall be proactive so as to reduce the occurrence of terrorist attacks.[92] This proactive approach to counter terrorism, also referred as precautionary approach, aims at preventing terrorist attacks, which includes the use of SITs to counterterrorism.[93] UNCTOC encourages states to cooperate in the investigation of transnational organized crimes by using SITs. [94]

Despite their positive contribution in preventing terrorist attacks, SITs are also susceptible to be abused or misused by law enforcement organs that would raise human right concerns.[95] This concern is further exacerbated because the advancement in science and technology has increased the intrusiveness of surveillance techniques.[96]

The right to privacy is one of the fundamental human rights that are adversely affected by the intrusive utilization of SITs. [97] Though ICCPR does not provide its definition, the right to

---

Terrorism, 'Basic Human Rights Reference Guide: Conformity of National Counter-Terrorism Legislation with International Human Rights Law' (2014) 10.

[89] 'Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa, General Principles-C& Part 13, Human Security (A) < https://caert.org.dz/official-documents/human_rights.pdf> accessed 25 Oct 2023; Ben Golder & George Williams, 'Balancing National Security and Human Rights: Assessing the Legal Response of Common Law Nations to the Threat of Terrorism'(2006) 8(1) Journal of Comparative Policy Analysis: Research and Practice 43, 49; CTITF Working Group (n 88) 3.

[90] Digest of Jurisprudence of the UN and Regional Organizations, (n 87) 12.

[91] Principles and Guidelines on Human and Peoples' Rights, (n 89) General Principles, Part 6, Criminalization and Sanctioning of Terrorism-A; Duffy (n 35) 25.

[92] UNODC Handbook on Criminal Justice (n 1) 5.

[93] ibid; UNODC(Crime Terrorism Prevention Branch) Preventing terrorist acts: A Criminal Justice Strategy Integrating Rule of Law Standards in Implementation of United Nations Anti-Terrorism Instruments' (2006) 2.

[94] United Nations Conventions on Transnational Organized Crimes, Art 20.

[95] Council of Europe Recommendations (n 43) preamble, para.13, Eijkman, and Weggemans (n 16) 143; Eijkman (n 16) 90; Worku (n 9) 84&94; Paolo (n 19).

[96] Melissa Cawthra, 'Collateral Intrusion: Safeguarding Privacy in an Age of Surveillance Guidelines for South Africa's Information Regulator (2020) APCOF research paper Series 1&2 < https://apcof.org/wp-content/uploads/apcof-research-29-privacy-and-surveillance-web.pdf> accessed Oct 2023; Paolo (n19) 202&204&205.

[97] UNODC Current Practice in Electronic Surveillance (n 56) 8; Cawthra(n 96) 4&9; Sobol *et al* (n 77) 8.

privacy can be taken as "a general protection of the individual from unreasonable observation of behaviors in private spaces."[98]

The adverse impact that SITs posed on the right to privacy is because such techniques enable law enforcement organs and security agencies to have access to personal and sensitive details of someone's life; in a way that erode the distinction between public and private life.[99] The use of video surveillance and wiretapping enables police and security agencies to trespass the traditional physical barriers protecting individuals privacy and observe people's private life; without the risk of being noticed.[100]

Infiltration through the use of undercover agents and criminal informants has also the potential to violate the right to privacy as it involves "the covert manipulation of a relationship in order to obtain information that may result in interference with the right to private and family life."[101]

Furthermore, governments may also use surveillance technologies indiscriminately against the whole or larger section of a civilian population.[102] Indiscriminate use of SITs entails unnecessary and disproportionate adverse impact on human rights because it, among others, brings individuals who are not terrorist risk under state's surveillance.[103]

The adverse impact that the utilization of SITs would pose to human rights is not only limited to the right to privacy. Other human rights like the right to freedom of expression, freedom of movement, right to assembly, freedom from discrimination would also be affected; because the fear of surveillance and interception discourages individuals not to properly exercise these rights.[104]

---

[98] John Hardy, *The Rise of the Modern Intelligence State*, (Counter-Terrorism, Ethics and Technology Emerging Challenges at the Frontiers of Counter-Terrorism, Adam Henschke et al eds. 2019) 109.

[99] Murray Hunter, 'Cops and Call records Policing and Metadata Privacy in South Africa' (2020)A report for the Media Policy and Democracy Project, 7-9 <https://www.researchgate.net/publication/342078824_Cops_and_call_records_Policing_and_metadata_privacy_in_South_Africa> accessed 2 Nov 2023; John Hardy (n 98) 107.

[100] Paolo(n 19) 205.

[101] Organization for Security and Co-operation in Europe(OSCE) and Office for Democratic Institutions and Human Rights (ODIHR), 'Human Rights in Counter-Terrorism Investigations, A Practical Manual For Law Enforcement Officers', (2013) 41< https://www.osce.org/files/f/documents/5/f/108930.pdf> accessed 1 Nov 2023.

[102] Cawthra(n 96) 9; Hardy(n 98) 107; Sobol *et al* (n 77) 8.

[103] Hardy(n 98)114; Sobol *et al* (n 77) 9.

[104] Cawthra (n 96) 9; OSCE and ODIHR(n 101) 32; Sobol et al (n 77)8.

CHAPTER THREE

3 PRE-CONDITIONS ON THE USE OF SITs IN COUNTER-TERRORISM

Though SITs are helpful in the prevention and prosecution of serious crimes including terrorism, adequate safeguards are also necessary to avoid the adverse impact that the use of such techniques would cause on the right to privacy and other human rights.[105] In this respect, counterterrorism measures shall be used in accordance with states' obligations under international human rights law.[106]

This makes it important to put in place a system that balances the positive attributes of SITs with the negative outcomes that the use of such techniques entail in the enjoyment of human rights.[107] This balance is maintained by setting preconditions that shall be met to use SITs.[108] According to the pre-conditions, the use of SITs to counter-terrorism is justified only in exceptional circumstances and as a matter of last resort.[109] The use of such techniques "….by law enforcement is commonly regulated by a warrant-based system, subject to some form of oversight."[110]

Different international and regional human rights and counter-terrorism instruments contain provisions setting preconditions on the use SITs. As the focus of this research is the use of SITs in counter terrorism in Ethiopia, some of the relevant international and domestic legal frameworks are discussed in the following sub-sections.

[105] OSCE and ODIHR (n 101) 33; Mahmood Rajpoot, Q., & Jensen, C. D, *Video Surveillance: Privacy Issues and Legal Compliance'* (V. Kumar, & J. Svensson (eds.), Promoting Social Change and Democracy through Information Technology IGI global) (2015) 1-2.
[106] See for instance, UN General Assembly Resolution, A/RES/68/167, Adopted on 18 December 2013.
[107] Worku (n 9) 94.
[108] OSCE and ODIHR (n 101) 32.
[109] UNODC Handbook on Criminal Justice, (n 1) 54; UNODC the Current Practice in the Use of Electronic Surveillance (n 56) 1; OSCE and ODIHR(n 101) 32.
[110] UNODC the Current Practice in the Use of Electronic Surveillance (n 56) 13 ; Cawthra (n 96) 14.

3.1 International Covenant on Civil and Political Rights (ICCPR)

The right to privacy is one of the human rights recognized under the Universal Declaration of Human Rights (UDHR)[111] and International Covenant on Civil and Political Rights(ICCPR)[112] Art 17 of the ICCPR states the following regarding the right of privacy.

1) No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks.

The protection from unlawful or arbitrary interference that ICCPR accorded to the right to privacy includes interferences coming from state authorities, natural and legal persons.[113] However, since the right to privacy is not an absolute right, it can be limited, among others, for detecting, preventing and investigating crimes including terrorism[114] Nevertheless, ' interference ….can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the covenant.'[115]

Accordingly, one of the preconditions that shall be fulfilled to interfere with the right to privacy is the presence of specific law authorizing the same. As per this provision, any interference with

[111] Universal Declaration of Human Rights(UDHR), UN General Assembly Resolution 217 A (1948) Art 12 < https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 23 Oct 2023.
[112] International Covenant on Civilian and Political Rights (ICCPR), General Assembly resolution 2200A (XXI) (1966) Art 17< https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights >accessed 23 Oct 2023.
[113] Human Rights Committee, General Comment No. 16, Article 17 , 'The right to respect of privacy, family, home and correspondence, and protection of honour and reputation,' (1988) para 1< https://www.refworld.org/docid/453883f922.htm l > accessed 26 Oct. 2023.
[114] UN General Assembly, Report of the Special Rapporteur of the Human Rights Council on the Right to Privacy, A/72/540, A report submitted in accordance with Human Rights Council resolution 28/16, P.4) para. 7 < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/335/64/PDF/N1733564.pdf?OpenElement > accessed 26 Oct. 2023; Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37 (2009) para. 15< https://policehumanrightsresources.org/content/uploads/2022/04/Sp-Rap-on-counter-terrorism-the-right-to-privacy.pdf?x49094 > accessed 26 Oct. 2023.
[115] General Comment No. 16 (n 113) para. 3.

the right to privacy including through the use of SITs would be 'unlawful' and/or 'arbitrary' in so far as not authorized by law.[116]

In addition, interferences in the right to privacy authorized by law 'shall be ….reasonable in the particular circumstances."[117] The interference is said to be reasonable only when it is necessary and proportional to achieve the objective envisaged by the law and the least intrusive one form the available alternatives.[118] Even in the existence of authorizing law, interfering with the right to privacy can still be 'arbitrary' if it is not necessary and not helpful to realize legitimate objectives.[119] Because of their impacts that interfere with the right to privacy, the necessity and proportionality measures apply to SITs too.[120]

Furthermore, the decision to take such measures interfering with the right to privacy shall be made by an 'authority designated by the law and on case by case basis.'[121] In this respect, the law recognizing the interference shall contain details rules, among others, identifying the authorized organ, the procedures of authorization and the time limits on the duration of the interference.[122]

3.2 African Charter on Human and Peoples Rights (ACHPR) and other African Counter-Terrorism Instruments

In the African context, the failure of the 'African Charter on Human and Peoples Rights (ACHPR) to recognize the right to privacy is taken by some to argue as to the inadequacy of law

[116] ibid.
[117] ibid, para. 4.
[118] The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights, Human Rights Council Twenty-seventh session Agenda items 2 and 3 Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A/HRC/27/37 para. 23. < https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/088/54/PDF/G1408854.pdf?OpenElement > accessed 25 Oct 2023.
[119] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37 (2009) para 17 < https://policehumanrightsresources.org/content/uploads/2022/04/Sp-Rap-on-counter-terrorism-the-right-to-privacy.pdf?x49094 > accessed 26 Oct. 2023.
[120] The UNGA (resolution 68/167) states about the use of surveillance, interception and data collection that adversely affect human rights, like the right to privacy. The resolution also reiterates the unlawful and arbitrary use of such techniques violates, among others, the right to privacy that protected under that the UDHR and ICCPR. As the resolution recommends for counter-terrorism measures to be implemented in accordance with international human rights laws, the legality, necessity, proportionality preconditions to interfere with the right to privacy also apply for SITs. (See UN General Assembly Resolution, A/RES/68/167 , The right to privacy in the digital age, on 18 December 2013, preamble and para 4 (a)-(d) < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/PDF/N1344947.pdf?OpenElement > accessed 9 Dec 2023.
[121] General Comment No. 16 (n 113) para 8.
[122] The Right to Privacy in the Digital Age (n 118) para. 28.

to safeguard this right from the arbitrary use of investigation techniques.[123] Nevertheless, the pre-conditions stipulated in ICCPR to interfere with individual's right to privacy are also applicable in the African states that have already ratified the ICCPR.[124]

In addition, though 'OAU Convention on the Prevention and Combating of Terrorism' impose an obligation to prevent terrorism, its provisions shall not be interpreted in a way that derogates from general principle of international law.[125] The OAU conventions also explicitly recognizes principles of international law and the UN General Assembly resolutions number 49/60 and 51/210.[126] Since UN General Assembly resolutions recommends for taking counterterrorism measures in accordance with international standards of human rights[127], it can be argued that the pre-conditions and safeguards on the use of SITs to counter-terrorism are also applicable in relation to 'OAU Convention on the Prevention and Combating of Terrorism' and its application in Africa. Ethiopia signed this convention on 24/09/1999, ratified it on 24/02/2003 and deposited its instrument of ratification on 05/03/2003.[128]

Moreover, the 'African Principles and Guidelines on Terrorism and Human Rights'[129] is the other useful regional counterterrorism instrument (soft law) that can be used as a basis to ensure counterterrorism measures compatibility with human rights. Accordingly, counter-terrorism measures limiting human rights shall be taken in exceptional circumstances to be provided by specific law, based on the proportionality and necessity requirements, to achieve the objectives of regional and international human rights laws.[130]

In particular, counter-terrorism measures interfering on the right to privacy, "…shall be provided for by law, strictly proportionate with and absolutely necessary for achieving a legitimate goal…"[131] Such measures shall be undertaken subject to judicial review and with a possibility

[123] Duffy (n 35) 36.
[124] ibid.
[125] OAU Convention (n 4) Art 22(1).
[126] ibid, preamble, para. 4.
[127] See for instance, UN General Assembly Resolution 49/60, Annex , para. 5.
[128] See <https://au.int/sites/default/files/treaties/37289-sl-oau_convention_on_the_prevention_and_combating_of_terrorism_1.pdf > accessed on 8th Nov 2023.
[129] African Principles and Guidelines on Terrorism and Human Rights, African Commission on Human and Peoples' Rights, (May 2015) 56th Ordinary Session < https://caert.org.dz/official-documents/human_rights.pdf> accessed 26 Oct. 2023.
[130] ibid, General Principle-M.
[131] ibid, Part-11, Right to Privacy-A.

to challenge the legality of such measures before the court of law. [132] Because of their intrusiveness towards the right to privacy, these preconditions also apply for SITs to counterterrorism because of their intrusiveness towards the right to privacy.

3.3 The FDRE Constitution

Fundamental human rights are protected under Chapter III of the FDRE Constitution. In addition, international treaties (including human right treaties) ratified by Ethiopia are part and parcel of Ethiopian law.[133] The fundamental rights enshrined under the constitution shall be interpreted in line with the UDHR and international human rights covenants and instruments adopted by Ethiopia.[134]

The fundamental human rights guaranteed under the constitution and international human rights instruments also include those ensuring the procedural fairness in criminal justice. 'All government organs at all levels shall have the responsibility and duty to respect and enforce Chapter III of the constitution'.[135] The human rights recognized therein and other instruments ratified by Ethiopia cannot be limited, during criminal justice administration, unless in accordance with the relevant provision of the constitution or the covenant.[136] This includes criminal justice responses to counter-terrorism including the implementation of SITs.

The right to privacy is the constitutional human rights that can be mentioned in relation to SITs to counter-terrorism. The FDRE constitution protects the right to privacy which includes the right to be free from search of home, body and property.[137] The constitution also recognized the inviolability of correspondence and communications on telephone or any other electronic means.[138]

In addition, the constitution provides under what grounds interference with the right to privacy is permitted. On this Art 26(3) of the constitutions reads as;

---

[132] ibid.
[133] Proclamation of the Constitution of the Federal Democratic Republic of Ethiopia (FDRE Constitution), Proclamation No. 1/1995 Fed *Negarit* Gazette, 1st Year No. 1) Art 9(4).
[134] ibid, Art 13(2).
[135] ibid, Art 13(1).
[136] Wondwossen Demissie, Human Rights and Criminal Process in Ethiopia, (Centre for Human Rights, Addis Ababa 2021).
[137] FDRE Constitution (n 133) Art 26(1).
[138] ibid, Art 26(1).

> …..No restrictions may be placed on the enjoyment of such rights except in compelling circumstances and in accordance with specific laws whose purposes shall be the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others.[139]

The above mentioned constitutional provision contains the preconditions that shall be met before taking measures restricting on the human right to privacy including through the use of SITs. These preconditions are the legality, proportionality and necessity requirements.

The first precondition is the requirement of legality, which requires the existence of specific law that authorizes the restriction of the right to privacy.[140] When this is brought to the use of special investigation techniques, there must be specific legislation that authorizes law enforcement organs to use such techniques while combating terrorism. The absence of this precondition to use SITs in counterterrorism holds the activities of law enforcement organs as illegal and even unconstitutional.

Secondly, restriction on the right of privacy may be placed only when there are compelling circumstances.[141] According to the necessity precondition, SITs shall not be used unless there are circumstances necessitating their use and they shall be used as a matter of last resort.[142] The prerequisite as to the existence of ' compelling circumstances' stated under Art 26(3) of the FDRE Constitution is a reiteration of the necessity precondition that shall be fulfilled to take measures interfering with the right to privacy, which is also applies for SITs to counter-terrorism.

Thirdly, the restrictions on the right to privacy shall not be imposed unless it is for the purposes of protecting "...national security or public peace, the prevention of crimes or the rights and freedoms of others…"[143] This is an element as to the existence of social interest to limit the right to privacy, which also include the proportionality requirement in the use of SITs interfering with the right to privacy.

---

[139] ibid, Art 26(3).
[140] ibid.
[141] ibid.
[142] The Right to Privacy in the Digital Age (n 118) para. 23.
[143] FDRE Constitution (n 133) Art 26(3).

3.4 SITs under the Prevention and Suppression of Terrorism Crimes Proclamation

3.4.1 The Preconditions to Employ SITs

In the PSTCP the preconditions to use SITs are prescribed under the different sub-provisions of Art 42.

> Police may use the following special investigation techniques if an act of terrorism has a serious damage to the country and public, where in the regular Criminal Procedure Code investigation technique is not effective to gather evidence regarding investigation of terrorism crime.[144]

Art 42(1) incorporates the necessity and proportionality preconditions that shall be fulfilled to the use of special investigation techniques. Accordingly, SITs shall be used only when ordinary investigation techniques are not sufficient to realize the objective of the criminal investigation[145], which shows that SITs are choices of last resort, justified based on necessity. In addition, the crime under investigation shall be a crime of terrorism of serious magnitude damaging to the public interest.[146] This is a proportionality requirement that SITs shall not be used to investigate crimes of less serious nature, even when the ordinary investigation techniques are not adequate to conduct the investigation.

In addition, the use of SITs requires prior court authorization which shall be granted when "the court believes the necessity of the use of special investigation techniques."[147] And the court shall evaluate the necessity based on the preconditions stated under Art 42(1) of the PSTCP. In the application of the PSTCP, the courts having jurisdiction to issue warrant authorizing the use of SITs are the Federal High Court of Ethiopia and Regional Supreme Courts.[148] In urgent conditions, the authorization to use SITs can be given by the head of public prosecutor; provided that the permission will be subjected to court approval within 48 hours.[149]

[144] PSTCP (n 26) Art. 42(1).
[145] ibid.
[146] ibid.
[147] ibid, Art. 42(2).
[148] ibid, Art. 39(1) (a).
[149] ibid, Art. 42(3).

The court issuing warrant on the implementation of SITs shall also be specific as to the type of technique to be used and how it shall be used.[150] The warrant shall not be given for more than ninety days[151], but the duration in each case shall be fixed to the extent that is only adequate to achieve the objective. Up on good cause and with proper oversight on the performance of the police officer, the court may also grant additional time, which shall not be more than thirty days.[152]

3.4.2 Empowered Institution to Use SITs

Under the PSTCP the responsibility to investigate crimes is given to Federal Police.[153] Specific to SITs, the mandate to use SITs is given to police up on the fulfillment of the preconditions specified under the law.[154] Though their prime objective is not evidence gathering for criminal conviction, in the experience of other countries, SITs can also be used by security agencies.[155] The authority of NISS to use SITs can also be raised in the PSTCP. In this respect, the PSTCP stated the role of NISS as follows.

> The National Intelligence and Security Services **shall follow up Terrorism Crime within the scope of Power and Functions given under its establishment Proclamation** and shall recruit and assign from among its employees for this purpose. Where necessary, organize a special work unit.[156] (emphasis mine)

Specific to counter terrorism, its establishment proclamation specifies that NISS has 'the power and the duty to investigate and follow up terrorism ….and collect intelligence and evidence.'[157] Its re-establishment proclamation states the following, regarding the mechanisms that can be employed by NISS to follow up crimes, including terrorism.

---

[150] ibid, Art 42(4).
[151] ibid, Art 42 (7).
[152] ibid, Art 42(7).
[153] ibid, Art 36(1).
[154] ibid, Art 42(1).
[155] Kenth Roath, 'The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relationship between Intelligence and Evidence' (2010) 4 The Unique Challenges of Terrorism Prosecutions 26.
[156] PSTCP (n 26) Art 42(7).
[157] National Intelligence and Security Service Re-establishment Proclamation (NISS Re-establishment Proclamation) Proclamation No 804/2013 (Fed *Negarit* Gazette, 19th Year No. 55) Art 8(3) Since the responsibility to investigate terrorism has already given to Federal Police by latest law(PSTCP), the mandate that NISS has in counterterrorism is only limited to following up.

> In order to protect national security and prevent threats to national security, **conduct surveillance**, **in accordance with court warrant**, on any person suspected of criminal activities referred to under sub-article 1,3,4,5 or 6 by entering in to any place **and by employing various mechanisms**.[158] (emphasis added)

Surveillance is one of the SITs recognized under the PSTCP,[159] the mandate that is given to NISS, by its establishment proclamation, to conduct surveillance shows that it's authorized to employ SITs to follow up terrorism suspects.

Nevertheless, since the provision specifically mention 'surveillance', questions can be raised as to whether NISS can lawfully use other SITs like interception. Here the phrase in Art 8(7) above that reads'...various mechanisms' is opened ended accommodating other SITs that can be used to follow up terrorism. In addition, intercepting communications is one way to conduct surveillance in counter-terrorism.[160] Since, the 're-establishment proclamation' doesn't provide a specific definition for the term 'surveillance'; it can be defined in wider manner as 'the collection or monitoring of information about individual/individuals through the use of technology.'[161] Thus, so long as the requirement on court warrant is fulfilled, NISS can use other SITs to follow up terrorism suspects.

[158] ibid, Art 8(7).
[159] PSTCP (n 26) Art 42 (1)(a)&(b).
[160] Lentini (n 48) 4&5.
[161] UNODC the Current Practice in Electronic Surveillance (n 56) 4-5.

CHAPTER FOUR

4 SITs IN COUNTER-TERRORISM IN ETHIOPIA: THE PRACTICE

Reviewed Cases

This chapter examines the implementation of the law on the SITs in counter-terrorism in Ethiopia. It draws on, real court cases decided by the Federal High Court of Ethiopia (hereafter referred also as the court) and by the Ministry of Justice, prosecution division.

But here, as doing otherwise is not within the scope of the research, the anti-terrorism court cases are used without evaluating, in their merit, as to whether the charges and the details thereof can really constitute a crime of terrorism, in the proper sense of the term.

4.1 Court Cases

From the total of 52 court cases that the Federal High Court has entertained as per the PSTCP, 35 cases have been reviewed with a view to see if evidences obtained through SITs have been used. In doing so, anti-terrorism charges containing documentary evidences labeled as "technically collected evidences/ technical investigation reports" prepared by NISS were chosen, as they are the only cases that related to SITs. As the technical investigation reports do not explicitly specify the techniques used to collect evidence, only those cases that the court makes reference to SITs in its judgment/ ruling are included in Table-I, by presuming that the court shall specify about SITs while summarizing the evidences in its judgments as per Art 149(1) of the CPC.

Table-I

Year	Total No of anti-terrorism cases decided	total number of files reviewed	number of files involving special investigation techniques	The type/s of special investigation techniques employed	Numbers of cases, proof of court authorization were presented.	Numbers of cases, proof of court authorization were not presented.	Evidences presented directly as they are obtained	Number of cases SITs were employed by NISS	Number of cases SITs were employed by Police
2020/ 21 (2013 e.c)	8	6	3 * [162]	Intercepting phone communication	0	3	0	3	0
2021/22 (2014 e.c)	18	12	2 ** [163]	Intercepting phone communication	0	2	0	2	0
2022/-23[164] (2015 e.c)	26	17	1 ***[165]	Intercepting phone communication	0	1	0	1	0

* *Endalkachew Robi vs. Federal Prosecutor; Dejene Serbesa Terfasa and Lelisa Gadissa Regassa vs. Federal Attorney General ; Bizuayehu Amente Geleta et al vs. Federal Prosecutor*

** *Hanbissa Gonfa Sima vs. Federal Prosecutor; Alem Desta Hayelom vs. Federal Prosecutor*

*** *Elleli Eni Robi et al vs. Federal Prosecutor*

In all of the cases listed under Table-I, the Federal Prosecutor presented technical investigation reports as documentary evidences against the accused persons.[166] These documentary evidences

[162] *Endalkachew Robi* vs. *Federal Prosecutor*, Federal High Court File No 266630 , (27 July 2021); *Dejene Serbesa Terfasa and Lelisa Gadissa Regassa vs. Federal Attorney General* , Federal High Court File No- 255296 (9 March 2021); *Bizuayehu Amente Geleta et al (Nine individuals) vs. Federal Prosecutor*, Federal High Court File No 255065 (4 June 2021).

[163] *Hanbissa Gonfa Sima vs. Federal Prosecutor*, Federal High Court File No 263421, (3 Dec 2021); *Alem Desta Hayelom vs. Federal Prosecutor*, Federal High Court File No 266554 , (13 Oct 2021) . In the latter case, through the accused was charged for "Outrages against the Constitution or the Constitutional Order" in violation of Art 32(1)(a) (b) and Art 238 (1)(b)& 238 (2) of the Criminal Code of Ethiopia, one of the documentary evidence presented against the accused was a technical investigation report prepared by NISS as per Art 37 (1) of the PSTCP.

[164] This figure represents the data only up to June 2023.

[165] *Elleli Eni Robi et al (Eight individuals) vs. Federal Prosecutor*, Federal High Court File No 298022, (12 April 2023).

[166] In the criminal charges, the prosecutor used two Amharic expressions namely "**የቴክኒክ ማስረጃ**" and "**በቴክኒካል የተሰበሰበ ማስረጃ**" interchangeably to refer the report prepared by NISS. As it is observed from the court cases, NISS stated the following while sending the technical investigation report to Ethiopian Federal Police. " **በወንጀል በተጠረጠሩት……..ላይ ማስረጃ እንድንልክ ጠይቃችሁናል፡፡ በመሆኑም የሽብር ወንጀልን ለመከላከል እና ለመቆጣጣር በወጣው አዋጅ** 1176/2012፣ **አንቀፅ** 37(1) **መሰረት በተጠርጣሪዎች ላይ በቴክኒካል የተሰበሰበ….ገፅ ማስረጃ መላካችንን እንገልፃለን**". Thus, in the context of this research, 'technical

on “technically collected evidences” were prepared by NISS based on the information gathered according to Art 37(1) of the PSTCP. In all of these cases, the court stated in its judgment or ruling that the evidence mentioned in the technical investigation report was obtained by intercepting phone communications.[167]

Though Police can use SITs in accordance with the preconditions stated under the PSTCP[168], the Ethiopian Federal Police has not yet started to use SITs by its own to investigate crimes of terrorism.[169] There are is no antiterrorism court case that can show police use of SITs to gather the evidences.[170] No request for cooperation has also been presented by Ethiopian Federal Police to ‘Ethiopian-telecom’, to investigate terrorism crimes by intercepting communications.[171] All these show that Ethiopia Federal police is not using SITs to counter terrorism.

As such, Table-I and other similar court cases[172] show that the use of SITs in Ethiopia has been dependent on NISS sharing technical investigation reports to Federal Police.[173]

---

investigation report’ is defined as a document prepared by NISS that summarizes and/or analyzes the ‘technically collected evidences’ obtained against the person/s suspected for terrorism crimes and later on submitted by the Federal Prosecutor as documentary evidence against the accused.

[167] See *Endalkachew Robi vs. Federal Prosecutor*, ruling given on 27 July 2021, p. 14; *Dejene Serbesa Terfasa and Lelisa Gadissa Regassa vs. Federal Attorney General* , ruling given on 9 March 2021, p.21 -22*; Bizuayehu Amente Geleta et al vs. Federal Prosecutor*, ruling given on 4 June 2021, p. 17-18 ; *Hanbissa Gonfa Sima vs. Federal Prosecutor*, judgment given on 17 May 2021, p. 20; *Alem Desta Hayelom vs. Federal Prosecutor*, ruling given on 13 Oct 2021, p. 4; *Elleli Eni Robi et al vs. Federal Prosecutor*, ruling given on 12 April 2023, p.6 &7

[168] See, PSTCP (n 26) Art 42-43.

[169] Interview with Anonymous, Anti-Terrorism Investigator, Ethiopian Federal Police (9 Oct 2023) at the office of the investigator, Ethiopian Federal Police Crime investigation Unit; Interview with Seid Kemal, Federal Prosecutor ,Ministry of Justice (12 Oct 2023) at the office of the Prosecutor, Ministry of Justice (*Lideta* Brach) See also **ፍትሕ ሚኒስቴር፣ የሽብር ወንጀልን ለመከላከልና ለመቆጣጠር የወጣ አዋጅ ቁጥር** 1176/2012 **አፈጻጸምን ለመገምገም የተደረገ የዳሰሳ ጥናት፣ ገፅ** 13.

[170] Interview with anonymous Investigator (n 169); Interview with Federal Prosecutor(n 169).

[171] Interview with Manaye Abera, Director, Ethiopian -telecom, Criminal cases Follow-up and Justice Support Unit (6th September 2023) at *Ethio-telecom* Head Office.

[172] *Wega Taddese Gerbeso vs. Federal Prosecutor* , (Federal High Court File No – 266613, (Jan, 2022); *Mohammed Eba Marra et al. (six individuals) vs. Federal Prosecutor*, Federal High Court File No- 292770, (March, 2023); *Birru Tuffa Elmo vs*. Federal Prosecutor, Federal High Court File No 266136 (Aug, 2022); *Abdissa Angessa et al (Three individuals) vs. Federal Public Prosecutor*, Federal High Court File No 254983, (June, 2021*); Aman* Assefa et *al (nine individuals) vs Federal Prosecutor* , (Federal High Court File No 266361, (28 June, 2022).

[173] **የዳሰሳ ጥናት** (n 169) 13 &21.

4.2 Federal Prosecutor Files

When it comes to cases in the FDRE Ministry of Justice, from the total of 59 Criminal investigation files that were closed by the prosecutor under Article 42 of the CPC, 44 files have been reviewed in order to identify cases that are related to evidence obtained through SITs. For the purpose of maintaining consistency, the anti-terrorism criminal investigation files which involve documentary evidences labeled "technically collected evidences/ technical investigation reports" are selected. As the technical investigation reports do not explicitly specify the techniques used to collect evidence, from these files, those that the prosecutor stated in its decision as to the existence of SITs mentioned in Table-II**.**

Table-II

Year	Total number of anti-terrorism investigation files closed	The total number of files reviewed	The total number of files involving special investigation techniques	The type/s of special investigation techniques employed	The total number investigation files containing proof of court authorization	The total number investigation files without court warrant	Evidence presented directly as they are obtained
2020/21 (2013 e.c)	3	2	0	-	-	-	
2021/22 (2014 e.c)	17	11	1*	Intercepting phone communication	0	1	0
2022/-23 (2015 e.c)	39	31	2**	Intercepting phone communication	0	2	0

** Anonymous, Federal Prosecutor File Number -517/15(Federal Police File No-883/14).*

*** Anonymous, Federal Prosecutor File No - 376/15 (Fed Police File No, 622/15), Anonymous, Federal Prosecutor File No- 216/15 (Federal Police File No- 761/14).*

Here it should be stated that, based on the request of the Federal Prosecutor the name of the suspects above and in the rest of this thesis is kept anonymous.

4.3 Court Authorization to Use SITs

As noted, the Ethiopia Federal Police has never used SITs by its own for counter-terrorism investigations.[174] It follows that this sub section is concerned with SITs employed by NISS.

In none of the court cases referred under Table-I and other cases[175] using technical investigation reports, is there a proof presented to show that court authorization was obtained prior to using the SITs. In three cases the court queried if court warrant was obtained. In *Hanbissa Gonfa Sima vs. Federal Prosecutor*[176], *Alem Desta Hayelom vs. Federal Prosecutor* [177] , *Bizuayehu Amente Geleta et al vs. Federal Prosecutor*[178] the prosecutor did not comply with the court order to present the copy of the court warrant. And in *Ambissa Angessa Teresa et al. vs Federal Prosecutor* case [179] NISS, without acknowledging the existence of interception, informed the court that the evidence was obtained with court warrant. However, when ordered to present the court warrant NISS declined from submitting its copy.[180]

Likewise, court warrants authorizing the use of SITs cannot also be found in the cases referred under Table-II and other criminal investigation files[181] containing technical investigation reports. According to the interviews conducted in this research, unwillingness of NISS to hand over the court warrants is the reason why the court warrants couldn't be presented as evidence in anti-terrorism cases and investigation files.[182]

---

[174] Interview with Investigator (n 169), Ethiopian Federal Police; Interview with Federal Prosecutor (n 169) see also **ፍትሕ ሚኒስቴር፣ የሽብር ወንጀልን ለመከላከልና ለመቆጣጠር የወጣ አዋጅ ቁጥር** 1176/2012 **አፈጻጸምን ለመገምገም የተደረገ የዳሰሳ ጥናት** (unpublished),13.

[175] *Wega Taddese Gerbeso vs. Federal Prosecutor* , Federal High Court File No – 266613, (Jan, 2022); *Mohammed Eba Marra et al. (six individuals) vs. Federal Prosecutor*, Federal High Court File No- 292770, (March,2023*); Birru Tuffa Elmo vs. Federal Prosecutor*, Federal High Court File No 266136 (August, 2022); *Aman Assefa et al (nine individuals) vs. Federal Prosecutor*, Federal High Court File No 266361, (June, 2022).

[176] Federal High Court File No 263421.

[177] Federal High Court File No 266554.

[178] Federal High Court File No 255296.

[179] Federal High Court File No 254983.

[180] The absence of the officer in possession of the court warrant in his/her office was the reason presented by NISS as an excuse not to present the copy of the court warrant.

[181] Federal Prosecutor File No 424/14; Federal Prosecutor File No 366/15; Federal Prosecutor File Number 290/15; Federal Prosecutor File No 375/15; Federal Police File No 621/15; Federal Prosecutor File No 361/15, Federal Prosecutor File Number 290/15; Federal Prosecutor File No 424/14. (Based on the request of the Federal Prosecutor, the name of the suspects in these files are kept anonymous)

[182] Interview with Anonymous (n 169); Interview with Federal Prosecutor (n 169).

In case of doubt concerning the legality of the evidence, the onus to prove the legality of the evidences falls on the side of the state.[183] And hence, if interception of phone communication and surveillance was indeed employed in the above mentioned cases, the unavailability of the copies of court warrant; coupled with the unwillingness of NISS to furnish the same when requested/ordered can lead to conclude that the evidences were obtained without prior court authorization.

[183] Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa,(n 129) Part 4. Right to Fair Trial , C(iii)).

CHAPTER FIVE

5 COMPATIBILITY OF THE LAW AND THE PRACTICE RELATING TO THE USE OF SITs IN COUNTER-TERRORISM PROSECUTIONS

5.1 The Requirement of Court Warrant

As noted, the legality of SITs can be ascertained based on the existence of specific legal framework recognizing the implementation of SITs with respect to a certain class of crimes. Furthermore, even in the existence of specific legislations authorizing the use of special investigation techniques, the legality of the evidences obtained through SITs shall also be ascertained by examining whether the investigation was conducted by complying with the procedures prescribed under the specific legislation. In this respect, police and Public Prosecutors have a responsibility to ensure that SITs are implemented lawfully.[184]

Evidences obtained in the absence of basic procedural guarantee or in a serious violation of human rights shall not be used as evidence in any proceedings.[185] As this also including the use SITs, evidences obtained without court authorization will be inadmissible in criminal proceedings. Moreover, if doubts as to the legality of the evidence are raised by the accused, the burden of proof to show the legality of the evidences falls on the side of the state.[186]

In the Ethiopia case, the PSTCP doesn't explicitly state the effect that noncompliance with court authorization entails on the admissibility of evidence. But still, the FDRE Constitution guaranteed the right to privacy together with the permissible grounds over which this right can be restricted. One of the preconditions is the existence of specific law like the PSTCP that authorizes the restriction of the right to privacy.[187] Unless in urgent cases specified under Art 42(3) of the PSTCP, prior court authorization is mandatory to use SITs.[188] Noncompliance with

[184] UNODC Handbook on Criminal Justice (n 1) 54.
[185] Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa (n 129) Part 4. Right to Fair Trial , C(i)); Principles and Guidelines on the right to fair trial and Legal Assistance in Africa< https://archives.au.int/bitstream/handle/123456789/2065/Right%20to%20a%20Fair%20Trial_E.pdf?sequence=1&isAllowed=y.> accessed 1 Nov 2023 ; UNODC Current Practices in Electronic Surveillance (n 56) 14.
[186] Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa (n 129) Part 4. Right to Fair Trial, C(iii).
[187] FDRE Constitution (n 133) Art 26(3).
[188] PSTCP (n 26) Art 42 (1).

this requirement will make the activities of law enforcement organs as illegal and unconstitutional that shall in turn hold the evidences obtained inadmissible to the case.[189]

The Ethiopian Criminal Justice Policy also prescribes for the relevant law to clearly state that illegally obtained evidences are inadmissible and if there are exceptional circumstances to hold them admissible, it shall be clearly stated under the Criminal Procedure Code.[190] Under the FDRE Criminal law Procedure and Evidence Code (Draft), court authorization is one of the preconditions to use SITs.[191] And failure to comply with this requirement makes the evidences obtained inadmissible. [192]

However, court cases show divergent practices on the effects of the absence of prior authorization to use SITs for counter-terrorism investigation. In some cases, the court has properly examined the legality of the evidences, by questioning the presence of court warrant authorizing the interception of phone communications. In these cases, the absences of proof of court warrant lead to the court to declare the evidences as illegally obtained and therefore inadmissible.

On the other hand, there are also cases showing the court's failure to examine the legality of the interception and admit the evidences without asking for proof showing the existence of court authorization prior to the employing the interception. The same divergent practice is also observed on the side of the Federal Prosecutor while passing decisions to prosecute or not prosecute.

[189] But this is not to mean that the court shall, in all circumstances, declare evidences gathered without court authorization inadmissible to the case. Though it shall be specified in the law/s, in certain exceptional circumstances, the court should have discretion to hold evidence obtained without court authorization admissible to a given case. For instance, in the experience of other countries the exclusion of illegally obtained evidence is left to the judge's discretion that will be decided by employing 'balancing test' ; by considering , among others, the kind/nature of constitutional right violated, the gravity of the crime, the mental state of the law enforcement organs while obtaining the evidence(whether it is intentional, negligent, by mistake ,by accident etc.), the public interest, the nature of the evidence, adverse impact on the reputation of the judiciary, the right to fair trial of the accused . (see, Stepen C. Thaman and Dominik Brodowski, *Exclusion or Non-Use of Illegally Gathered Evidence in the Criminal Process: Focus on Common Law and German Approaches* (Core Concepts in Criminal Law and Criminal Justice, Kai Ambos et al eds. Cambridge University Press , 2019) 437- 440.

[190] The Federal Democratic Republic of Ethiopia Criminal Justice Policy (2015) 26.

[191] Criminal Law Procedure and Evidence Code of the Federal Democratic Republic of Ethiopia (Draft), Art 104 (1)-(3).

[192] ibid Art 107 & Art 260 (b).

5.1.1 The Court Practice

A. Cases the Court Properly Examined the Legality of the Evidence

As it is mentioned earlier under Chapter-4 of this research, there is no instance whereby the prosecutor presented proof of court authorization together with the criminal charge. [193] And the court followed two types of approaches before passing its verdict on the legality of (the interception) and admissibility of the evidences .

The first approach shows a relatively lenient stand of court. As such, even if the court warrant is not presented together with the criminal charge, the court will still give a chance for the Federal Prosecutor to present the court warrant.[194] For instance, in *Hambissa Gonfa vs. Federal Prosecuor*[195], *Bizuayehu Amente Geleta et al vs. Federal Prosecutor*[196] the prosecutor was ordered to submit the court warrant that authorized the gathering of evidence by intercepting phone communications. In these cases the order was given after the trial of the case has already been started. In the former case, the statement given by the court says " ….even if the evidence [court warrant] is expected to be presented together with the criminal charge, the prosecutor was ordered to present the same on due course of the proceeding….."[197] This shows the relaxed stand of the court as to when the court warrant authorizing the interception of phone communication shall be presented.

In *Bizuayehu Amente Geleta et al vs. Federal Prosecutor* case, the prosecutor's failure to present the copy of court warrant made the court to assume that the interception was conducted illegally without court authorization. In its judgment the court stated that;

> There is no evidence presented by the prosecutor to prove that NISS has ……obtained the evidences in accordance with the constitution and other subsidiary legislation. This

[193] Table –I and interview with W/*ro Haregwoin Teklu* and *Ato Kassaye Zerihun*, Federal High Court Judges (03 August 2023) at the Judges Office Federal High Court(*Lideta* Branch). The judges also mentioned an improvement in the practice in this respect. Here, the judges referred one pending anti-terrorism case; the court warrant authorizing the interception was presented together with the criminal charge. (The authorization was given by Federal High Court, *Arada* branch, Remand bench in File number 009413).
[194] Interview with judges, ibid.
[195] Federal High Court File No 263421.
[196] Federal High Court File No 255296.
[197] ibid.

> shows that…. the evidence was illegally obtained without fulfilling the requirements stated in subsidiary legislation and by violating the constitution.[198]

This coupled with the prosecutor's failure to present the intercepted communications directly as they are obtained made the court to declare the technical report prepared by NISS inadmissible and acquit the accused as per Art 141 of the Criminal Procedure Code.

On the other hand, the second approach shows strict stand of the court. Unlike the first approach, the failure of the prosecutor to present the copy of the court warrant will automatically lead the court to assume that the evidence is illegality obtained. It is without giving a chance for the prosecutor to present the court warrant that the court would give this conclusion. In this respect, the judgments that the court rendered in *Alem Desta Hayelom vs. Federal Prosecutor*[199], and *Dejene Serbesa Terfasa and Lelisa Gadissa Regassa vs. Federal Attorney General*[200] , *Endalkachew Robi vs. Federal Prosecutor*[201]can be mentioned.

The above mentioned cases show the proper role that the court has played in scrutinizing the legality of evidences obtained through interception phone communications and disregarding evidences that are collected without securing prior court warrant to that effect.

B. Cases Showing the Court's Failure to Examine the Legality of the Evidence

Despite the existence of cases where the court played its proper role in examining the legality of evidence contained in technical investigation reports prepared by NISS, there are also cases where the court failed to do so.

In *Wega Taddese Gerbeso vs. Federal Prosecutor,*[202]the court admitted technical investigation reports summarizing the communications and information that the accused was alleged to have exchanged with member of a proscribed terrorist organization. Even though court warrant authorizing the gathering of evidence was not presented together with the criminal charge, the court admitted the report, without ordering the prosecutor to submit the copy of the court warrant, and sentenced the accused for five years of rigorous imprisonment.

---

[198] ibid.
[199] Federal High Court File No - 266554.
[200] Federal High Court File No - 255296.
[201] Federal High Court File No - 266630.
[202] Federal High Court File No – 266613.

In *Aman Assefa et al (nine individuals) vs. Federal Prosecutor*[203] the court against admitted technical investigation reports on the phone communication that the accused allegedly had in furtherance of committing the crimes of terrorism. In this case too, without scrutinize the legality of the evidence the court sentenced the accused for different present terms ranging from 5 years and 6 months up to 3 years and 4 months of rigorous imprisonment.

C. Court's Approach to Evidence NISS Collected through SITs

In cases referred under Table-I, the court stated that interception of communication have been used to gather the evidences mentioned in the technical investigation reports. However, such conclusion of the court can be criticized because of the following reasons.

In all of the cases except one, the court did not provide the reason why it concluded that NISS had used interception of communications to obtain the evidences.[204] And in *Alem Desta Hayelom vs. Federal Prosecutor* case the court stated the following regarding its assumption as to the use of SITs to gather evidences presented against the accused.

> The contents of the report presented by NISS, on evidences claimed to have been obtained technically based Art 37(1) of the PSTCP, indicate that the evidences were obtained by using special investigation techniques (phone interception).[205] (translation mine)

However, even in this case, the court failed to show how and which contents of the technical investigation report indicate the presence of phone interception to gather the evidence. In view of that other types of SITs like infiltration and surveillance could have been used by security agencies, including NISS, to follow terrorism suspects the court's approach is questionable. And hence, while technical investigation reports did not say anything as to the method of evidence gathering it will be unwarranted for the court to conclude interception of phone communication without providing the reasons that made it to draw such assumptions.

---

[203] *Aman Assefa et al (nine individuals) vs. Federal Prosecutor* , (Federal High Court File No 266361, (25 June 2022).

[204] The interview conducted with the High Court Judges doesn't also give sufficient justification as their response they did not properly differentiate evidences gathered through forensic investigation on cellphones from evidences obtained through interception of phone communications.

[205] Federal High Court File No -266554.

The other drawback in the court judgments is the lack of consistency in stating the techniques that NISS used to gather evidences. For instance, technical investigation reports prepared by NISS were also presented in *Wega Taddese Gerbeso vs. Federal Prosecutor* [206] , *Mohammed Eba Marra et al. vs. Federal Prosecutor*[207] , *Birru Tuffa Elmo vs. Federal Prosecutor*[208] , *Abdissa Angessa et al vs. Federal Public Prosecutor*[209] and *Aman Assefa et al vs. Federal Prosecutor.*[210] Unlike the cases referred in Table-I, in these cases the court said nothing regarding the technique that was utilized to gather the evidences that was used to prepare the technical investigation reports.

5.1.2 The Practice in the Federal Prosecutor

A. Inconsistent Practices of the Prosecutor

The PSTCP has empowered the Attorney General to lead the investigation of terrorism crimes and conduct court litigations.[211] As part of this role, the Federal Prosecutor has a responsibility to ensure that SITs are implemented lawfully and with court warrant before instituting criminal charges. Nevertheless, in cases referred under Table-I and other cases,[212] using technical investigation reports as evidence, the Federal Prosecutor filled criminal charge without having the copy of court warrant given to NISS to collect evidence/information through SITs.

Whereas, in the cases referred under Table- II and other similar investigation files [213] containing technical investigation reports prepared by NISS, the Federal Prosecutor properly examined the presence of the copy of court warrant authorizing the use of SITs; the absence of which is stated as one of the reasons to pass decision not to prosecute the suspects as per Art 42(1)(a) of the CPC.

---

[206] Federal High Court File No-266613.
[207] Federal High Court File No-292770.
[208] Federal High Court File No-266136.
[209] Federal High Court File No-254983.
[210] Federal High Court File No-266361.
[211] PSTCP (n 26) Art 38 1 (a).
[212] *Wega Taddese Gerbeso vs. Federal Prosecutor , Mohammed Eba Marra et al. vs. Federal Prosecutor , Birru Tuffa Elmo vs. Federal Prosecutor , Abdissa Angessa et al vs. Federal Public Prosecutor and Aman Assefa et al vs. Federal Prosecutor.*
[213] Anonymous suspects in Federal Prosecutor File No 424/14, Federal Prosecutor File No 366/15, Federal Prosecutor File Number 290/15, and Federal Prosecutor File Number 290/15.

B. Prosecution's Approach to the Evidence NISS collected through SITs

The criminal investigation files referred under Table-II contain technical investigation report prepared by NISS summarizing and/or analyzing the communications that the suspected individuals had by using phone numbers to commit the crimes of terrorism for which they were suspected. In these cases too NISS did not explicitly specify the method that was used to gather the evidences.

Despite this, in its decision not to institute criminal proceeding before court of law the Federal Prosecutor' stated that interception of phone communication to have been used to obtain the evidences contained in the technical investigation report. Though the prosecutorial decisions did not provide any information as to how the prosecution knew interception was used, the prosecutors would consider the reference made to specific phone numbers to assume that the evidences are obtained by intercepting phone communication.[214] In addition, the prosecutor also added that had other methods been used to gather evidences , NISS would have stated it clearly in the report; just like reports prepared by conducting forensic investigations on electronic devices (cellphone, laptops etc) found in the hands of the suspects at the time of their arrest.[215]

Nevertheless, as phone numbers/ phone communications can also be used while employing other SITs like infiltration and criminal informants, the reference in the technical investigation reports to specific phone numbers /phone communications *per se* cannot be a conclusive proof as to the presence of phone interception to obtain the evidences stated in the technical investigation report.

5.2 The Requirement of Presenting Materials Obtained through the SITs Directly

In the previous Anti-Terrorism Proclamation (ATP) the admissibility of hearsay and intelligence reports that do not disclose the source and methods used to gather information entailed outcomes militating against fair trial rights of the accused persons.[216] But under the PSTCP 'evidences

[214] Interview with Federal Prosecutor (n 169).
[215] ibid. In the anti-terrorism investigation on *Degaga Tariku et al* (Federal Prosecutor File Number 182/15) NISS stated the following while sending a report prepared based on forensic investigation " **በእነ ደጋጋ ታሪኩ በተጠረጠሩበት የሽብር ወንጀል መረጃ እንድንልክ ጠይቃችሁናል። በመሆኑም የሽብር ወንጀልን ለመከላከል እና ለመቆጣጠር በወጣው አዋጅ ቁጥር** 1176/2012 **አንቀፅ** 37 **መሰረት በተጠርጣሪዎች ላይ በፎረንሲክ የተሰበሰበ** (**ከኤሌክትሮኒክስ መሳሪያዎች ላይ የተገኙ**).....**ገፅ መላካችን እንገልፃለን።** " (emphasis mine)
[216] Amerti (n 25) 143.

obtained through interception by national or foreign law enforcement organs shall not be valid where they are not presented directly as they are obtained.'[217] Thus, in the case of anti-terrorism prosecutions under the PSTCP, evidences obtained by interception shall be presented by submitting the direct audio record as it is[218] or in case of written communications, by presenting the written text directly as it is.

There are practical reasons that can be presented to justify why Art 42(6) of the PSTCP shall be strictly complied with. For instance, evidences obtained through SITs may be altered which raise concerns on their reliability.[219] This risk will be pronounced if technical investigation reports are to be relied on while the evidences are not presented directly as they are obtained.

In some anti-terrorism investigations, the contents of forensic investigation reports prepared by NISS were not matching with the actual contents of the evidences when they are presented directly as they are obtained. For instance, in one criminal investigation file case[220] , individuals were suspected of supporting a proscribed terrorist organization. NISS conducted forensic investigation on the electronic devices owned/possessed by the suspects to uncover the communications that they had through short text messages and on different social media platforms. Though the report produced by NISS alleged that the suspects committed the crime, the Federal Prosecutor found out that the report prepared by NISS was not matching with the evidences directly presented as they are obtained. On this point the decision not to prosecute passed by the prosecutor reads as follows.

> Forensic investigation has been conducted on the cellphones of the suspects. The communications that they had on short message communications ….and on other social media platforms was presented and analyzed in the report; in a way that shows the suspects have something to do with the crime that they were suspected for. Nevertheless, the evidence directly presented in printed form and CD proved nothing in relation to the crimes they are suspected for.[221] (translation mine)

[217] PSTCP (n 26) Art 42(6).
[218] Amerti (n 25) 143.
[219] Paolo (n 19) 202.
[220] Anonymous , Federal Prosecutor File No - 376/15, Federal Police File No- 622/15.
[221] ibid.

In addition, in another criminal investigation file [222] , the prosecutor stated that the contents of the investigation report, describing and analyzing the evidence extracted from the cellphone and Facebook accounts of one of the suspects, did not much with the actual contents of the evidence presented directly as it is obtained.

If the above mentioned mismatches were seen in forensic investigations reports prepared by NISS, their possibility cannot also be ruled out in other reports prepared based on evidences obtained through SITs.

But here, the fact that Art 42(6) of the PSTCP talks only about evidences obtained by interception shall not be interpreted in a way that doesn't require evidences obtained through other SITs to be presented directly as they are obtained. In view of that the provision is introduced to safeguard the right to fair trial[223],by ensuring their right to access to evidence, it would make sense to argue that evidences obtained by other SITs, like video and photo surveillance, shall also be presented directly as they are obtained. Because Art 42(6) of the PSTCP holds evidence that are not presented directly as they are obtained inadmissible, intelligence reports that are prepared based on the evidences obtained through SITs (without presenting the evidence directly as it is obtained) shall also be taken as inadmissible.

Though the PSTCP doesn't provide a definition for the term 'intelligence', the NISS Re-establishment proclamation' defines it as;

> Information helpful to protect and defend the national security of the country and collected analyzed and prepared by the National Intelligence and Security Service to provide to the appropriate government bodies.[224]

In the court cases referred under Table-I and other cases[225] , technical investigation reports prepared by NISS, based on information obtained while following up individuals who were potential terrorism suspect, were presented as evidence against the accused persons. These technical investigation reports are the summary and analysis of the communications that the

[222] Anonymous , Federal Prosecutor File No 424/14, Fed Police File No 384/14.
[223] Amerti (n 25) 143.
[224] NISS Re - establishment Proclamation (n 157) Art 2(3).
[225] *Wega Taddese Gerbeso vs. Federal Prosecutor , Mohammed Eba Marra et al. (six individuals) vs. Federal Prosecutor , Birru Tuffa Elmo vs. Federal Prosecutor , Abdissa Angessa et al (three individuals) vs. Federal Public Prosecutor , Aman Assefa et al (nine individuals) vs. Federal Prosecutor.*

accused allegedly had over the phone to plan and/or prepare to commit terrorism crimes or assist the perpetration of the crime. As the technical investigation reports did not specifying the source and techniques used to gather the information, the information stated therein is mere 'intelligences' which in turn makes the technical investigation reports no different from intelligence reports. In fact, technical investigation report can be taken as euphemism for intelligence reports.

Evidences that are obtained through SITs are not admissible in anti-terrorism criminal trials unless they are presented directly as they are obtained.[226] But the actual court cases show the existence of inconsistency in holding technical investigation reports inadmissible. While in some cases the court held technical investigation reports inadmissible, in others it did not.

5.2.1 The Court Practice

A. Cases the Court held Technical Investigation Reports Inadmissible

In *Endalkachew Robi vs. Federal Prosecutor*[227] and *Alem Desta Hayelom vs. Federal Prosecutor,*[228] the Federal Prosecutor presented, among others, technical investigation report prepared by NISS summarizing the preparations and/ or communications that the accused allegedly had by using phone numbers in furtherance of the crimes that they were accused for.

After stating as to utilization of interception to gather evidences, the court ordered the prosecutor to present the audio record of the intercepted communications. Nevertheless, the prosecutor didn't present the audio record as ordered. In *Endalkachew Robi vs. Federal Prosecutor* case the direct audio record was not presented because it is said to be designated as 'top secret' by the Director General of NISS; because revealing the same entails prejudicial outcomes on national security by compromising future anti-terrorism follow ups that will be undertaken. But in *Alem Desta Hayelom vs. Federal Prosecutor* case, no justification has been presented not to submit the audio-records.

[226] PSTCP (n 26) Art 42(6).
[227] Federal High Court File No-266630.
[228] Federal High Court File No-266554 .

In both cases, the court cited Art 42(6) of PSTCP to hold the technical investigation reports inadmissible and acquitted the accused without the need to defend them. In particular, the court commented the following in *Endalkachew Robi vs. Federal Prosecutor* case.

> Proclamation No 1176/2020 obliges that evidences obtained through interception by law enforcement organs shall not be valid where they are not presented directly as they are obtained. After NISS claimed that it has found evidences against the accused by intercepting phone communication and presented the same in written form, the allegation as to the adverse impact that submitting the direct audio record would cause on national security is not lawful justification.[229] (translation mine)

In *Bizuayehu Amente Geleta et al vs. Federal Prosecutor*[230] technical investigation reports prepared by NISS were presented as documentary evidence against the accused. In this case too, the court stated that the reports were prepared based on evidences obtained by intercepting phone communication.[231] Even if the criminal charge was presented based on the provision of the PSTCP, the technical investigation report was prepared based on the ATP. Despite this, the court evaluated the admissibility of the technical investigation report in accordance with the provisions of the PSTCP. After being ordered to submit the audio-record of the intercepted communication, the prosecutor was not able to present the same, as the court declared the technical investigation report inadmissible which is one of the reasons to acquit the accused without the need to defend him.[232]

B. Cases the Court held Technical Investigation Reports Admissible

There are anti-terrorism cases, contrary to its position in the above discussed cases, where the court admitted technical investigation reports as evidence against the accused. In *Aman Assefa et al vs. Federal Prosecutor* case[233] the accused were charged in three different counts for preparation to commit a terrorist act in violation of Art 32(1)(a) of the Criminal Code and Art 6(2) of the PSTCP ; for membership in terrorist organization named ISIS in violation of Art

[229] Federal High Court File No-266630.
[230] Federal High Court File No-255296.
[231] Up on filling the criminal charge, the Federal Prosecutor would list/present technical investigation reports as documentary evidences. For more explanation see foot note remark number 166 above.
[232] For more on similar approach by the court see: *Elleli Eni Robi et al vs. Federal Prosecutor* (Federal High Court File No- 298022.
[233] Federal High Court File No- 266361.

30(1) of the PSTCP and preparation to commit a terrorist act in violation of Art 32(1)(a), Art 37 of the Criminal Code and Art 6(2) of the PPPSTC.

In this case the Federal Prosecutor presented documentary evidences against the accused. One of the documentary evidence was a technical investigation report prepared by NISS. This report contains the summary of the communication that the accused allegedly had on phone communication by using different phone numbers. The other documentary evidence was also prepared by NISS, based on the evidences extracted through forensic investigation conducted on laptops and other electronic devices seized from some of the defendants.

Since five of accused denied the charge presented against them, the court considered the documentary evidences including the technical investigation report prepared by NISS to order the accused to start their defense. In doing so, the court did not consider whether the communication that the accused allegedly had over phone calls is presented in the same way as they are obtained.

In their defense, some of the accused requested, among others, for the direct audio-record of the alleged phone communications to be presented. Even if the court ordered NISS to present the audio-record, the latter did not comply with the court order claiming that the said evidence is designated as 'a top secret' by the Director General of NISS.

In this case, the fact that the court used the technical investigation report to order the accused to defend themselves by itself show that the court admitted the report as evidences against the accused, despite that the item of 'evidence' is not that envisaged under Article 42(6) of the Proclamation, without letting the accused to have access to the evidence presented against them, thereby compromising their right to get fair trial.

Moreover, the court's failure in safeguarding the accused right is further magnified when it accepted the justification presented by NISS not to submit the direct audio-records of the phone conversation. In particular, the court commented the following to reject the objection raised by the defense lawyers and convicted the accused.

> The court does not have the legal basis to order the lawful response and information presented [by NISS] to be changed in accordance with the application of the accused. Thus, the petition [of the accused] is rejected.[234] (translation mine)

Furthermore, in *Wega Taddese Gerbeso vs. Federal Prosecutor*[235] case, the accused was charged under Art 32(1)(a), 35 and 38 of the FDRE Criminal Code and Art 3(2) of the PSTCP for committing a terrorist act. One of the documentary evidences presented by the prosecutor was a technical investigation report prepared by NISS that summarized the communications and information that the accused exchanged with members of a proscribed terrorist organization called *Shene* through two specifically identified phone numbers.

In this case, when the court altered the criminal charge to Art 3 (1) (d) and (e) of the PSTCP and ordered the accused to start his defense, it did not say anything as to the admissibility of the technical investigation report. And since the accused couldn't defend himself, the court passed a guilty verdict (by majority vote) and sentenced the accused for five years of rigorous imprisonment. In doing so, the court referred the contents of the technical report prepared by NISS as a proof for the exchange of information/ communication that the accused was alleged to have had with members of a proscribed terrorist organization. This shows that the court has admitted the technical investigation report as evidence against the accused, without questioning why the phone communication alleged in the technical investigation report were not presented directly as they are obtained.

The adverse impact that the admissibility of the technical investigation report caused on the right to fair trial of the accused is visible; as he is sentenced for five years of rigorous imprisonment; while the rest of the evidences presented against him did not show the alleged communication between the accused and members of the proscribed terrorist organization. On this point the dissenting judge commented the following.

> The accused were arrested by NISS ….because he was suspected to have been delivering information to members of *Shene* and soliciting a member of Oromia

[234] ibid. While the court considered the response of NISS as 'lawful', it did not comment as to how admissible evidences shall be presented in accordance with Art 42 (6) the PSTCP.
[235] Federal High Court File No -266613.

Police to join *Shene*. But this accusation shall not be accepted as testimony given by the witness did not prove anything about it.[236]

5.2.2 The Practice in the Federal Prosecutor

The inconsistency in the use of technical investigation reports in also observed in prosecutorial decisions passed by the Federal Prosecutor. Thus, cases referred under Table-I and other cases[237] show the problem, on the Federal Prosecutor's side, in presenting technical investigation reports as evidences in anti-terrorism prosecution, without presenting the evidences directly as they are obtained. This is practice that is not in line with Art 42(6) of the PSTCP.

In the abovementioned cases, rather than presenting the technical investigation report as evidence, Federal Police and Federal Prosecutor should have undertaken further activities in order to change the intelligence in to admissible evidences that can be presented in criminal trials. In this respect, getting the intelligence that were stated in the report directly as they are obtained and getting the copy of the court warrant (to ensure the legality of the evidences) are some of the activities that should have been conducted to change intelligence to admissible evidence for criminal prosecutions[238].

The exclusive role that NISS is playing in the implementation of SITs coupled with NISS's unwillingness to give evidences directly as they are obtained are some the problems inhibiting the prosecutor not to present evidences obtained by interception directly as they are obtained.[239] In addition, inability of Ethiopian Federal Police to use SITs by its own is the other problem contributing for the misapplication of Art 42(6) of the PSTCP.[240]

As stated by the Federal Prosecutors, inability to get evidences directly as they are obtained has come to be an established norm that the Prosecutors have started to refrain from requesting such

---

[236] ibid.

[237] *Wega Taddese Gerbeso vs. Federal Prosecutor , Mohammed Eba Marra et al. (six individuals) vs. Federal Prosecutor , Birru Tuffa Elmo vs. Federal Prosecutor , Abdissa Angessa et al (three individuals) vs. Federal Public Prosecutor , Aman Assefa et al (nine individuals) vs. Federal Prosecutor.*

[238] According to Art 8(3) of 'NISS Re-establishment Proclamation', NISS has the duty to follow terrorism and collect intelligence and evidence. When this provision is read together with Art 8(7) of the same proclamation, NISS shall get court warrant to collect intelligence through surveillance and other intrusive techniques. Whether NISS has to secure court warrant to collect intelligence through infiltration remains unclear though.

[239] Interview, Federal Prosecutor (n 168); Interview, Federal Police Investigator (n 168). See also the **የዳሰሳ ጥናት** (n 169) 21.

[240] ibid.

type of evidences in every case.[241] In this respect, the decision not to prosecute given in one antiterrorism investigation file, in its relevant part reads as;

> Knowing how the information was obtained and getting the information directly and fully as they are obtained is important for prosecutorial decision. Nevertheless, it is established from previous practice that such types of evidences cannot be obtained. And hence, it is found to be necessary to evaluate the evidences through other means, without the need to ask NISS as to the direct contents of the information.[242]

As there are anti-terrorism criminal charges presented by the prosecutor by using technical investigation reports as evidence, there are also commendable prosecutorial decisions that are in line with Art 42(6) of the PSTCP. For instance, in criminal investigation files A[243], B[244] and C[245], the Federal Prosecutor decided not to prosecute the suspects because the information stated in the technical investigation report prepared by NISS were not presented directly as they are obtained.

5.3 The Secrecy *vs.* Disclosure Dilemma in Anti-terrorism Trials

Some of the cases discussed above demonstrated one of the challenges in criminal law measures to counter-terrorism *i.e.* the problem in using intelligence as evidence in anti-terrorism prosecutions.[246]

In old days, the line between intelligence and evidence used to be demarcated based on the difference in the mandates of security agencies and law enforcement organs. [247] As such, while

[241] See for instance, Anonymous (15 individuals), Federal Prosecutor File No 376/15; Anonymous (8 individuals) , Federal Prosecutor File No 375/15. The name of the suspects kept anonymous based on the request of the Federal Prosecutor.
[242] Anonymous (8 individuals), Federal Prosecutor File No-375/15.
[243] Anonymous (15 individuals), Federal Prosecutor File No-376/15.
[244] Anonymous (8 individuals), Federal Prosecutor File No-375/15.
[245] Anonymous (2 individuals), Federal Prosecutor File No-216/15.
[246] Leah West, 'The Problem of "Relevance": Intelligence to Evidence Lessons from UK Terrorism Prosecutions' (2018) 41 (4) Manitoba Law Journal 73.
[247] Roath (n 155) 22-24; West (n 246) 68; Quirine Eijkman & Bibi van Ginkel, 'Compatible or Incompatible? Intelligence and Human Rights in Terrorist Trials'(2011) 3(4) Amsterdam Law Forum 4.

security agencies used to have exclusive mandate in collecting intelligence in matters of national security; law enforcement organs would collect evidences for criminal proceedings.[248]

However, in counter-terrorism the above mentioned distinction between intelligence and evidence is obsolete because of the criminalization of inchoate conducts related to terrorism and the preventive role that police plays in counter-terrorism. As Alessandro Lentini stated it, the criminalization of preparatory acts and planning to commit terrorist acts results in 'the osmosis between criminal and intelligence investigation.'[249] Furthermore, the utilization of SITs by security agencies blurred the line between intelligence and evidence.[250] Intelligence agencies may also collect intelligence in a way that can be later used as evidence in criminal prosecutions.[251]

This blurring of distinction between intelligence and evidence brings challenges in anti-terrorism prosecutions. One of the challenges is maintaining fairness in the trial and at the same time keeping the secrecy of intelligence source and techniques; not to alert future offenders to change their techniques.[252] Disclosure of evidence obtained through SITs may also endanger the wellbeing of criminal informants and security agents.[253]

As noted above, in some cases, evidences were not presented directly as they are obtained because they are classified by the Director General of NISS as ' top-secret'. For instance, in *Endalkachew Robi vs. Federal Prosecutor,*[254] *Abdissa Angessa et al vs. Federal Prosecutor*[255] , *Tefferi Gerboshe Geletta et al vs. Federal Prosecutor*[256] *Aman Asseffa vs. Federal Public Prosecutor* [257] and *Birru Tuffa Elmo vs. Federal Prosecutor*[258] the direct audio record was not presented as it is said to be designated as 'top secret' by the Director General of NISS.

[248] Roath (n 155) 22-24; West (n 246) 68, Eijkman & Ginkel (n 247) 4&5.
[249] Lentini (n 48) 3.
[250] Roath (n 155) 25-26; West (n 246) 71.
[251] West (n 246) 63.
[252] Peter Sommer, 'Evidence from Hacking : A few Tiresome Problems' (2022) 40 Forensic Science International: Digital Investigation 1&3; West (n 246) 61 &73.
[253] OSCE and ODIHR (n 101) 32 &40- 42.
[254] Federal High Court File No-266630 .
[255] Federal High Court File No-254983.
[256] Federal High Court File No-249693.
[257] Federal High Court File No-266361.
[258] Federal High Court File No-266136.

As per the judges' experience in the Federal High Court of Ethiopia, justification based on classification as 'top-secret' is the only response that they know that would be presented when the direct audio-record of the alleged phone communication is demanded to be presented. [259] As per the opinion of the judges, the vagueness of the justification (simply asserting designation as top-secret) is open to abuse; because there is no additional evidence or document that would be presented to show that the specific audio-record ordered to be presented or audio records in general are indeed designated as top-secret.[260] On this point, the court commented the following in the ruling given in *Abdissa Angessa et al vs. Federal Prosecutor* case

> …….Even if the evidence is designated as top-secret by the Director General of NISS, there is no evidence that NISS presented to show that the required evidence is indeed designated as top-secret.[261] (translation mine)

Furthermore, the court also stated the following regarding the threat that submitting the audio record alleged to pose on national security.

> The claim that alleges submission of the audio-record will divulge the identity of the person and the techniques used to obtain the evidences is not acceptable; because it is not well explained to justify why and how the submitting of the evidence will lead to the occurrence the assumed risks.[262] (translation mine)

In some cases, the court went to the extent of questioning the appropriateness of classifying the evidences contained in the technical investigation reports presented against the accused as ' top-secret'. For instance, in *Abdissa Angessa et al vs. Federal Prosecutor,* the court commented the following to reject the justification presented by NISS.

[259] Interview with judges (n 193).
[260] ibid.
[261] Federal High Court File No- 254983.
[262] ibid.

> The audio record that NISS was ordered to present is the intelligence report that was formerly presented against the accused in public, which shows that the evidence is not a top-secret ….[263] (translation mine)

However, despite what the court has commented to reject the justification presented by NISS in *Abdissa Angessa et al vs. Federal Prosecutor* case , the most important thing is whether the law allows the court to admit technical investigation reports without requiring the evidence as obtained if the Director General designates it as 'top secret'. Under the PSTCP Art 42 (6) evidences that are not presented directly as obtained are inadmissible to the case irrespective of the designation as ' top-secret'.

In the case of evidence classified as secret, the state may decide to abandon anti-terrorism prosecutions.[264] In the case of the PSTCP, since it the responsibility of the Federal Prosecutor to present the evidences as required by the law, the prosecution shall be forfeited if the evidence is a classified as secret. And if the charge is filled only based on technical investigation reports, without presenting the evidences directly as obtained, the court shall declare the report as inadmissible as per Art 42 (6) of the PSTCP and dismiss the case.

This being said, while the court rejected the justification presented by NISS in the above mentioned cases, on the contrary in *Aman Assefa et al vs. Federal Prosecutor*[265] case the court accepted the justification by considering it as lawful.[266] This shows the existing dilemma in maintaining the balance between secrecy in intelligence and fairness in anti-terrorism trials in Ethiopian including those using evidence obtained by SITs.

To overcome the problem, a study conducted by Ministry of Justice recommended, among others, for NISS to inform Federal Police about the undergoing counter-terrorism follow ups so that the latter can secure court authorization and use interception of phone communication to gather evidence for future prosecutions.[267] Though the recommendation of the assessment study

---

[263] Federal High Court File No- 254983. But here, the court seem to have overlooked the fact that intelligence report can be prepared by disguising relevant details(including how the evidence is obtained) that NISS doesn't want to disclose, which would otherwise be revealed if the direct audio record is directly presented.
[264] West (n 246) 57-58&73.
[265] Federal High Court File No- 266361.
[266] For more on this see reference number 234 above.
[267] **የዳሰሳ ጥናት** (n 169) 13.

may have workable aspects, it can hardly be a solution in all times because of the following reasons.

First of all, the use of STIs including intercepting phone communication shall be authorized by the court up on the fulfillment preconditions stated under Art 42(1) of the PSTCP. In this respect, the receipt of information by Federal Police alone will not be sufficient enough to justify the request for court warrant to intercept phone communication.

Secondly, the time that NISS would communicate the outcomes of its follow-up to the Federal Police also matters. If NISS uses surveillance, which may also include interception of phone communications, to follow up terrorism, it shall do so by securing prior court authorization.[268] If NISS informed the Federal Police about the undergoing terrorism follow up and outcomes thereof, Federal Police's request for court authorization to use interception of communication, if succeeded means that NISS and Federal Police will continue to simultaneously use interception of phone to perform their respective mandates. And this will create unnecessary duplication of tasks between NISS and Federal Police.[269] In addition, the court authorization for Federal Police to use interception doesn't also always mean that NISS would not like to keep the audio-records as secret for national security reasons.

The last but not the list, the importance of the evidences collected by NISS till it informs Federal Police to start investigation shall also be considered. Police may not be able to get evidence even by using SITs which may be compelling to resort to the evidences collected by NISS to prosecute the suspects, provided that they obtained lawfully.

5.4 The Existing Investigation Gaps in Using SITs to Counter-terrorism

5.4.1 Establishing the Real Users of Mobile Phone Numbers

In all of the court cases that are studied in this research work containing technical reports prepared by NISS, the accused persons alleged to have used mobile phone numbers to communicate with other individuals in planning, preparing or executing the terrorism crimes.

[268] See NISS Re-establishment Proclamation (n 157) Art 8(7).

[269] In the experience of countries like Italy, preventive interception is implemented by ensuring the absence of unnecessary duplication of activities between law enforcement forces and intelligence agencies. (see Lentini (n 48)8) .

However, the Federal Police and Federal Prosecutor did not conduct further investigation to establish whether the suspected individuals (mentioned in the technical investigation report) were the exact persons who had the communications on the phone numbers.

As the court cases studied show, the evidence presented in this respect is only "Customer Acquisition Forms" obtained from *Ethio-Telecom*; showing the identity of the persons in whose name the phone numbers were registered. [270] But here, whether a certain mobile phone number was registered in the name of the accused/suspect or not, additional evidences are still necessary to establish the identity of the exact person who was using the phone numbers to communicate with other individuals in planning, preparing or executing the terrorism crimes. "Customer Acquisition Forms" alone cannot prove this fact beyond reasonable doubt because of the following reasons.

Firstly, the person in whose name the phone number is registered and the one who is actually using it might be two different individuals. Though "the customer shall not assign, transfer or sub-lease, the service without prior written consent of *Ethio-telecom*"[271] , individuals may still breach this prohibition and transfer phone numbers to another individuals. In addition, there were also instances showing phone numbers were purchased by individuals holding counterfeited documents (falsified identity cards) that belong to another person.[272] People using phone numbers registered in someone else's name is a commonplace practice.

As a result, the fact that one mobile phone number is registered in someone's name does not necessary mean that s/ he was the one using the same to commit the activities mentioned in the NISS technical investigation report. In *Elleli Eni Robi et al vs. Federal Prosecutor*[273], the court stated in its judgment as to the absence of evidence proving the accused was indeed using the mobile phone numbers mentioned in the technical report**.**

[270] However, there is no consistency in presenting "Customer Acquisition Forms" as evidence together with the criminal charge. As such, from the total of twelve court cases that are studied in this research, it is only in two cases namely, *Endalkachew Robi vs. Federal Prosecutor* and *Abdissa Angessa et al vs. Federal Public Prosecutor* that the prosecutor presented "Customer Acquisition Form" as evidence together with the criminal charge. And on the contrary, in *Elleli Eni Robi et al vs. Federal Prosecutor* , *Birru Tuffa Elmo vs. Federal Prosecutor* and *Tefferi Gerboshe Geletta et al vs. Federal Prosecutor* , the documentary evidences submitted by *Ethio-telecom* showed that the mobile phone numbers mentioned in the NISS's technical report were not registered in the name of the accused individuals.

[271] The Ethio-telecom 'Tele-communication Service Customer Agreement Form, *Ethio-telecom,* Art 12.

[272] Interview with Manaye Abera, (n 170).

[273] *Elleli Eni Robi et al (Eight individuals) vs. Federal Prosecutor* , Federal High Court File No- 298022.

As the Federal Prosecutor shall prove the charge beyond reasonable doubt, after receiving the report prepared by NISS, describing technically collected evidences, further investigations shall be conducted to get additional evidence as to whether the suspected individuals were indeed the exact persons who conducted the communication on the phone numbers.

Here, evidence proving the same is necessary even in the presence of the direct audio record of an intercepted communications which can be presented as evidence against the accused because the audio-record *per se* would prove little as to the identity of the person/s that is in the record. In this regard, conducting sound forensic investigation to draw match between the actual voice of the suspect/accused and the voice in the records of intercepted communications can be helpful to establish the requited link.[274]

5.4.2 The Importance of Using Additional Corroborative Evidences

The other investigation gap observed in relation to the use of SITs is the problem of presenting additional corroborative evidences. As observed from the cases that have been referred to write this research, the technical investigation report prepared by NISS mentioned diffident places / locations where the accused and/or other co-offenders were residing at the time when they had the alleged phone conversations to plan/prepare to commit terrorism crimes.

Nevertheless, despite what is stated in the technical investigation reports, there is no other evidence that can show the accused/s or other co-offender/s was physically present in the particular location/s and dates mentioned in the technical reports. Even in the presence the audio records of the intercepted phone communication, this gap would still make the evidences of the prosecutor open for alibi defenses. As a result, further investigation and evidence is necessary to get additional corroborative evidences that can fill this gap. In this regard, the experience of other countries show that getting location data from phone records can provide very useful corroborative evidence. [275]

Furthermore, other evidences that would assist the judges to understand the evidences shall also be presented together with the audio-record of intercepted communications. For instance, 'in the

[274] Fayyad-Kazan et al, 'Verifying the Audio Evidence to Assist Forensic Investigation' (2021) 14(3) (Computer and Information Science 2021) < https://www.researchgate.net/publication/353012073_Verifying_the_Audio_Evidence_to_Assist_Forensic_Investigation > accessed 8 Nov 2023.
[275] Hunter(n 99) 19.

interception of telephone calls…..conversations may involve non-standard language and accents that may be difficult for the listener to understand.'[276] In some anti-terrorism cases in Ethiopia the suspects/accused were heard while using code names to refer to grenades/explosives.[277] In addition, the judges have also commented the absence of sufficient evidences to infer the existence of 'communication' between the accused accused/s and other persons who are alleged to have been planning/ to perpetrate crimes of terrorism.[278]

To solve this problem, like in the case of South Africa, expert police witnesses may be used to present cellphone evidences to the court.[279] In addition, the technical investigation report prepared by NISS can also be admissible as corroborative evidences. Here, there is no associated fair trial concerns if verifiable information obtained through SITs are presented as evidence in anti-terrorism prosecutions.[280] And hence, so long as the evidence obtained through SITs is presented directly as obtained, the technical investigation report can be verified against the evidences. And the report will be helpful for the judges to properly understand what is being seen/ heard in the evidence presented directly as it is obtained.

[276] OSCE and ODIHR (n 101) 39.
[277] Interview with Federal Prosecutor (n 169).
[278] Interview, Judges (n 192) As per the opinion of the judges, 'communication' has three basic elements within it namely- 'encoder (መልእክት አመንጪ)', 'code (መልእክት)' and 'decoder (መልእክት ተግባሪ)'. The judges commented that there are not sufficient evidences to infer these three elements clearly in the actual criminal charges alleging phone communications between the accused and others who are suspected of plotting to commit crimes of terrorism. (also in *Gebregiworgis Gedey vs .Federal Attorney General*, Federal High Court Number 292170).
[279] Hunter (n 99) 16.
[280] Eijkman & Ginkel (n 247) 8.

CHAPTER SIX

6 CONCLUSION AND RECOMMENDATION

6.1 Conclusion

In counter terrorism, the use of is taken as part of a proactive approach to counter-terrorism that aims at preventing terrorism before they are actually committed. Though SITs are proven to be useful in the prevention and prosecution of terrorism crimes, they have also the potential to endanger fundamental human rights like the right to privacy.

As a result, the use of SITs shall be regulated by legal framework that balances security and protection of human rights. This balance is maintained by setting preconditions that shall be met to use SITs in counter terrorism. Accordingly, the use of criminal investigation techniques shall be recognized by specific law and they shall be used only exceptional circumstances based on the principles of necessity and proportionality. The use of such techniques shall be based on prior authorization from independent organ identified by the law.

In the Ethiopian experience, as observed from the real court cases and anti-terrorism investigation files, the practical implementation of SITs in Ethiopia is highly dependent on NISS sharing technical investigation reports to Federal Police. Though Police can use SITs in accordance with the preconditions stated under the PSTCP, the Ethiopian Federal Police has not yet started to practically use SITs by its own.

And regarding the practice in getting prior court authorization to use SITs, all the court cases and criminal investigation files that are studied in the research do not contain copy of court warrant showing the legality of evidence extraction. Nor were the prosecution able to produce copy of the court warrant in cases where they were ordered by the trial court. This can lead one to conclude that the SITs are being implemented without court authorization.

Furthermore even though the evidences obtained through SITs shall be presented directly as they are obtained, the practice is not compatible with the law. The designation of the evidence as ‘ top-secret ’ by the Director General of NISS is an impediment hindering the implementation of law.

In some cases, the court admitting technical investigation reports as evidence affected the accused right to fair trial as the accused were convicted without getting adequate opportunity to defend them. However, there are also commendable decisions showing the improvements that the court in safeguarding the rights of accused persons, by holding technical investigation reports inadmissible against the accused.

Furthermore, regarding status of evidence collected through SITs not supported by a court warrant, real court cases show a mixed practice in this respect. While the court in some cases properly scrutinize the legality of the evidence and declare those that are not supported by court warrant. And in some other cases, the court failed to properly examine the legality of evidence presented against the accused.

In addition, the focus of the prosecutor and investigation police is limited only to get the audio record of the intercepted communication, the investigation failed to gathering additional evidences like establishing the real users of mobile phone numbers and other corroborative evidences.

6.2 Recommendations

- For the proper implementation of the legal framework on SITs the Ethiopian Federal Police shall start to employ SITs by its own
- To resolve the dilemma on the interplay between fair trial and secrecy in anti-terrorism prosecutions, detailed legal framework on the evidence and intelligence exchange between NISS and Federal police shall be enacted.
- While using evidences obtained through SITs, corroborative evidences shall also be presented and Ethiopia Federal police shall improve its investigation skill and manpower to use other sources of evidence.
- Courts and Prosecutors shall adopt consistency in protecting the rights of the accused persons in terms of applying the rules on admissibility and legality of evidence obtained through SITs.

Bibliography

Laws

- The Constitution of the Federal Democratic Republic of Ethiopia, Proclamation No 1/1995 , Fed *Negarit* Gazette, Year 1, No 1 Addis Ababa, 21st August 1995
- Anti-Terrorism Proclamation, Proclamation No 652/2009, Fed *Negarit* Gazette, 15th Year No. 57, Addis Ababa 28th August, 2009
- National Intelligence and Security Service Re-establishment Proclamation, Procl No 804/2013 Fed *Negarit* Gazette, 19th Year No 55, Addis Ababa, 3rd July 2013
- The Prevention and Suppression of Terrorism Crimes Proclamation, Procl. No.1176/2020, Fed *Negarit* Gazette, 26th Year No. 20, Addis Ababa 25th , March 2020
- Computer Crime Proclamation, Procl No. 958/2016, Fed *Negarit* Gazette, 22nd Year No. 83

Book/ Book Chapters

- Brysk A., *Human Rights and National Insecurity , National insecurity and Human rights Democracies Debating Counterterrorism*, (Alison Brysk and Gershon Shafir eds. University of California Press 2007)
- Hardy J., *The Rise of the Modern Intelligence State* (Counter-Terrorism, Ethics and Technology Emerging Challenges at the Frontiers of Counter-Terrorism, Adam Henschke et al eds. 2019)
- Mahmood Rajpoot, Q., & Jensen, C. D, *Video Surveillance: Privacy Issues and Legal Compliance'* (Promoting Social Change and Democracy through Information Technology IGI global, V. Kumar, & J. Svensson eds.2015)
- Sailofsky D. and Shor E., *Human Rights and Terrorism: Issues and Overview* (International Human Rights and Counter Terrorism, Eran Shor and Stephen Hoadley eds. 2019)
- Thaman Stephen C. and Brodowski D., *Exclusion or Non-Use of Illegally Gathered Evidence in the Criminal Process: Focus on Common Law and German Approaches* (Core Concepts in

Criminal Law and Criminal Justice, Kai Ambos et al eds. Cambridge University Press, 2019)

- Vrailas C.B., *United Nations Human Rights Standards as Framework Conditions for Anti-Terrorist Measures* (Anti-Terrorism Measures and Human Rights, Wolfgang Bendek and Alice Yotopoulos-Marangopoulos eds,Maritinus Nijhoff Publishers 2004)
- Wondwossen D., *Human Rights and Criminal Process in Ethiopia*, (Centre For Human Rights, Addis Ababa University 2021)

Articles

- Amerti S., 'Appraising the Reform of the Anti-Terrorism Proclamation of Ethiopia Based on Applicable Human Rights Standards', XII Ethiopian Human Rights Law Series, (2020)
- Cawthra M. 'Collateral Intrusion: Safeguarding Privacy In An Age Of Surveillance', Guidelines For South Africa's Information Regulator, APCOF Research Paper Series, 2020)
- Dreher A., Gassebner M. and Siemers L.H, 'Does Terrorism Threaten Human Rights? Evidence from Panel Data', 53(1) The Journal of Law & Economics , (February 2010)
- Duffy H., 'Global Trends in Counter-terrorism Implications for Human Rights in Africa', Institute for Security Studies, Monograph 206 (March, 2023)
- Eijkman, Q. and Daan Weggemans D., 'Visual Surveillance and the Prevention of Terrorism: What about the Checks and Balances?', 25(3) International Review of Law, Computers & Technology (Nov.2011)
- Eijkman Q., 'Preventive Counter-terrorism and Non-discrimination Assessment in the European Union', 2 Security and Human Rights (2011)
- Eijkman Q. & Ginkel B., 'Compatible or Incompatible? Intelligence and Human Rights in Terrorist Trials', 3(4)Amsterdam Law Forum (2011)
- Ford J, 'African Counter-terrorism Legal Frameworks a Decade after 2001', Institute for Security Studies(ISS), Monograph 177 (March 2011)

- Golder B. & Williams G., 'Balancing National Security and Human rights: Assessing the Legal Response of Common Law Nations to The Threat Of Terrorism', 8(1) Journal of Comparative Policy Analysis: Research and Practice,(March 2006)

- Gross E. 'The Struggle of a Democracy against Terrorism -Protection of Human Rights: The Right to Privacy versus the National Interest - the Proper Balance', 37(1) Cornell International Law Journal (2004)

- Hiruy W. , 'The Right to Privacy in the Age of Surveillance to Counter Terrorism in Ethiopia', 18 African Human Rights Law Journal, (2018)

- Hunter M., 'Cops and Call Records Policing and Metadata Privacy in South Africa', A Report for the Media Policy and Democracy Project, (March, 2020)

- Michaelsen C., 'Balancing Civil Liberties against National Security? A Critique Of Counterterrorism Rhetoric', 29(2)UNSW Law Journal (2006)

- Paolo D. G., 'Judicial Investigations and Gathering of Evidence in a Digital Online Context', 80 International Review of Penal Law, (2009)

- Sobol, I., Moncrieff M, and Gaggioli G., 'Exploring Counterterrorism Effectiveness and Human Rights Law', WORKING PAPER, Geneva Academy of International Humanitarian Law and Human Rights (June 2023)

- Roath K., 'The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relationship between Intelligence and Evidence' 4 The Unique Challenges of Terrorism Prosecutions(2010)

- Stella M., 'Defining International Terrorism to Protect Human Rights', 29 Security And Human Rights (2018)

- Sommer P., 'Evidence from Hacking : A few Tiresome Problems', 40 Forensic Science International: Digital Investigation, (2022)

- West L., 'The Problem of "Relevance": Intelligence to Evidence Lessons from UK Terrorism Prosecutions', 41 (4) Manitoba Law Journal (Oct 2018)

- Wondwossen D., 'How to Rescue Human Rights from Proactive Counter Terrorism in Ethiopia', XXIX Journal Of Ethiopian Law (2017)
- Wondwossen D. , 'Court's Reluctance to Safeguard Rights of Accused in the Ethiopian Counter-terrorism Prosecutions and its Border Implications', 16(1) Mizan Law Review, (Sep. 2022)
- Worku Y., 'The Use of 'SITs and Tools' in the Fight against Serious Crimes: Legal Basis and Human Rights Concerns in Ethiopia', XXX Journal Of Ethiopian Law (2018)
- Yusuf S., 'The Resilience of the Human Rights Norm in an Era of Counter-Terrorism', UNISCI Discussion Papers, Nº 28, (January 2012)
- Zelealm K., 'The Terrorism of 'Counterterrorism': The Use and Abuse of Anti-Terrorism Law, the Case of Ethiopia', 13(13) European Scientific Journal (May 2017)

Online sources

- Council of Europe, The Deployment of Special Investigative Means, Criminal Asset Recovery Project in Serbia (2013) < https://rm.coe.int/deployment-of-special-investigative-means-eng/16807828fa >
- United Nations Office on Drugs and Crime (UNODC), Handbook on Criminal Justice Responses to Terrorism, Criminal Justice Handbook Series (2009)< https://www.unodc.org/documents/terrorism/Handbook_on_Criminal_Justice_Responses_to_Terrorism_en.pdf >
- UNODC, Current Practice in Electronic Surveillance in the Investigation and serious and organized Crimes < https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf >
- United Nations Office on Drugs and Crime(UNODC), University Module Series on Counter-terrorism, Module 12< https://www.unodc.org/e4j/zh/terrorism/module-12/introduction-learning-outcomes.html >

- Alessandro Lentini, Selected Issues in Counter-terrorism: special investigative techniques and the international judicial cooperation Focus on the European Union, (2019)< https://www.dirittopenaleglobalizzazione.it/wp-content/uploads/2018/03/Alessandro-Lentini-Selected-Issues-in-Counter-Terrorism.pdf >

- Nilsson H. G., Special Investigation Techniques and Developments In Mutual Legal Assistance - The Crossroads Between Police Cooperation and Judicial Cooperation, 125th International Training Course Visiting Experts' Papers, Resource Material Series No. 65< https://www.unafei.or.jp/publications/pdf/RS_No65/No65_07VE_Nilsson2.pdf >

- Organization for Security and Co-operation in Europe(OSCE) and Office for Democratic Institutions and Human Rights (ODIHR), Human Rights In Counter-Terrorism Investigations, A Practical Manual For Law Enforcement Officers, (2013) < https://www.osce.org/files/f/documents/5/f/108930.pdf >

- United Nations Office of the High Commissioner on Human Rights, United Nations Counter-Terrorism Implementation Task Force: CTITF Working Group on Protecting Human Rights while Countering Terrorism, Basic Human Rights Reference Guide: Conformity of National Counter-Terrorism Legislation with International Human Rights Law (October 2014), < https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/counterterrorismlegislation.pdf >

- 'Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa< https://caert.org.dz/official-documents/human_rights.pdf >

- Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa < https://archives.au.int/bitstream/handle/123456789/2065/Right%20to%20a%20Fair%20Trial_E.pdf?sequence=1&isAllowed=y >

- 13 International Principles on the Application of Human Rights to Communications Surveillance < https://www.eff.org/files/necessaryandproportionatefinal.pdf >

- Digest of Jurisprudence of the UN and Regional Organizations on the Protection Of Human Rights while Countering Terrorism <

https://www.ohchr.org/sites/default/files/Documents/Publications/DigestJurisprudenceen.pdf >

- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37 (2009) < https://policehumanrightsresources.org/content/uploads/2022/04/Sp-Rap-on-counter-terrorism-the-right-to-privacy.pdf?x49094 >

- Human Rights Committee, General Comment No. 16, Article 17 , 'The right to respect of privacy, family, home and correspondence, and protection of honour and reputation,' (1988) < https://www.refworld.org/docid/453883f922.html >

Other sources

- Criminal law Procedure and Evidence Code of the Federal Democratic Republic of Ethiopia(Draft)

- The Federal Democratic Republic of Ethiopia Criminal Justice Policy (2015)

- **የሽብር ወንጀልን ለመከላከል እና ለመቆጣጠር በተዘጋጀ ረቂቅ አዋጅ ላይ የተዘጋጀ አጭር ማብራሪያ**, (**በኢፌድሪ ጠቅላይ አቃቤ ሕግ፣ የሕግና ፍትሕ ገዳዮች አማካሪ ጉባኤ፣** 2012 **ዓ.ም**)

- **የሽብር ወንጀልን ለመከላከልና ለመቆጣጠር የወጣ አዋጅ ቁጥር** 1176/2012 **አፈጻጸምን ለመገምገም የተደረገ የዳሰሳ ጥናት፣(የፍትሕ ሚኒስቴር፣ ሐምሌ** 2014)

International/.Regional Instruments

- OAU Convention on the Prevention and Combating of Terrorism, 14 June 1999.

- UN Convention on Transnational Organized Crime (2000).

- 'Council of Europe Committee of Minsters Recommendations' "special investigation techniques" in relation to serious crimes including acts of terrorism, Rec(2005)10, Adopted by the Committee of Ministers on 20 April 2005 .

- The United Nations Global Counter-Terrorism Strategy, Resolution adopted by the General Assembly on 8 September 2006.

Court Cases

- *Alem Desta Hayelom vs. Federal Prosecutor*, Federal High Court File No- 266554 , (Nov 2021)
- *Aman Assefa et al (nine individuals) vs. Federal Prosecutor* , (Federal High Court File No 266361, (July 2022)
- *Abdissa Angessa et al (three individuals) vs. Federal Public Prosecutor*, Federal High Court File No- 254983, (July 2021)
- *Birru Tuffa Elmo vs. Federal Prosecutor*, Federal High Court File No- 266136 (August, 2022)
- *Bizuayehu Amente Geleta et al (nine individuals) vs. Federal Prosecutor*, Federal High Court File No- 255065 (June 2021)
- *Dejene Serbesa Terfasa and Lelisa Gadissa Regassa vs. Federal Attorney General* , Federal High Court File No- 255296 (March 2021)
- *Elleli Eni Robi et al (Eight individuals) vs. Federal Prosecutor*, Federal High Court File No 298022, (May 2023)
- *Endalkachew Robi vs. Federal Prosecutor*, Federal High Court File No -266630 , (Feb 2021)
- *Hanbissa Gonfa Sima vs. Federal Prosecutor,* Federal High Court File No- 263421, (Dec 2021)
- *Tefferi Gerboshe Geletta et al (Seven individuals) vs. Federal Prosecutor*, Federal High Court File No- 249693, (Nov 2021)
- *Mohammed Eba Marra et al. (Six Individuals*) *vs.* Federal Prosecutor, Federal High Court File No- 292770, (March 2023)

- *Wega Taddese Gerbeso vs. Federal Prosecutor* , Federal High Court File No - 66613, (Feb 2022)

Criminal Investigation Files

- Anonymous, Federal Prosecutor File No 375/15, Federal Police File No- 621/15.
- Anonymous, Federal Prosecutor File No- 361/15, Federal Police File No- 075/15
- Anonymous, Federal Prosecutor File No- 517/15, Federal Police File No -883/14
- Anonymous, Federal Prosecutor File No -290/15, Federal Police File No -635/14
- Anonymous, Federal Prosecutor File No- 290/15, Federal Police File No- 661/14
- Anonymous, Federal Prosecutor File No- 290/15, Federal Police File No- 854/14
- Anonymous, Federal Prosecutor File No- 366/15 , Federal Police File No- 585/15
- Anonymous, Federal Prosecutor File No -216/15, Federal Police File No- 761/14
- Anonymous, Federal Prosecutor File No- 376/15, Fed Police File No-622/15
- Anonymous, Federal Prosecutor File No- 424/14, Federal Police File No-328/14

Interviews

- W/ro Haregwoin Teklu , Federal High Court Judge (3 August , 2023)
- Ato Kassaye Zerihun, Federal High Court Judge, (3 August , 2023)
- Ato Manaye Abera, Ethiopian Telecom, Criminal and Justice Follow up Unit, Director (6 September ,2023)
- Anonymous, Ethiopian Federal Police Anti-terrorism Investigator (9 Oct, 2023)
- Seid Kemal , Federal Prosecutor, Ministry of Justice. (12 Oct, 2023)