ADDIS ABABA UNIVERSITY

College of Law and Governance Studies

School of Law

The Role of the Police in Protecting Human Rights against Technology-Oriented Crimes: the Case of Lideta Sub-City.

By: Bilisa Tamrat

GSE/8659/11

Advisor: Comdr.Demelash Kassay (PhD.Associate Professor)

September 2024

Addis Ababa

ADDIS ABABA UNIVERSITY

College of Law and Governance Studies

School of Law

The Role of the Police in Protecting Human Rights against Technology-Oriented Crimes: the Case of Lideta Sub-City.

A Thesis Submitted to Addis Ababa University, the School of Law: in Partial Fulfillment of the Requirements for the Degree of Masters of Laws in Law of Human Rights.

By: Bilisa Tamrat

Advisor: Comdr.Demelash Kassay (PhD.Associate Professor)

September 2024

Addis Ababa

Author's Declaration

I, Bilisa Tamrat, hereby declare that the thesis entitled 'The Role of the Police in Protecting Human Rights Against Technology-Oriented Crimes: In Case of Lideta Sub-City is my original work and that it has not been submitted for any degree or examination in any other University. I also pledge that all sources used in any form are duly acknowledged.

Bilisa Tamrat

Date: _____

Signature: _____

Advisor: Comdr.Demelash Kassay (PhD.Associate Professor)

Date _____

Signature _____

ADDIS ABABA UNIVERSITY

College of Law and Governance Studies

School of Law

Graduates Programs Board of Examiners

Thesis Approval Sheet

Bilisa Tamrat thesis, entitled as "The Role of the Police in Protecting Human Rights against Technology-Oriented Crimes: the Case of Lideta Sub-City." is approved by the undersigned members of the examining board.

Board of Examiners	Signature	Date
Advisor: Comdr.Demelash (PhD.Associate Professor)	_____	_____
Examiner 1: _____	_____	_____
Examiner 2: _____	_____	_____

ACKNOWLEDGEMENT

First and foremost, I want to thank God, followed by my family my mom and dad for their unwavering support. Without them, this would not have been possible. I also want to express my gratitude to my adviser, Comdr.Demelash Kassay (PhD.Associate Professor), whose expertise, guidance, and encouragement have been invaluable throughout this journey. His insightful feedback and dedication have inspired me to strive for excellence and have significantly enhanced the quality of this work and finally, I want to thank my husband for his continuous emotional support.

I would also like to extend my heartfelt thanks to the Lideta Police Office for their cooperation and willingness to participate in this research. The officers' valuable input and experiences have provided crucial insights into the challenges of combating technology-oriented crimes. Their candid responses and commitment to justice have greatly contributed to the depth and relevance of this study. I sincerely appreciate their time and effort in sharing their knowledge and perspectives.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ACHPR:	African Charter on Human and Peoples Rights
CFAA:	Computer Fraud and Abuse Act
DHS:	Department of Homeland Security
ECHR:	European Convention on Human Rights
ECPA:	Electronic Communications Privacy Act
EHRP:	Ethiopian Human Rights Project
FDRE:	Federal Democratic Republic of Ethiopia
GDPR:	General Data Protection Regulation
HOF:	House of Federation
HOPR:	House of Peoples Representatives
HRC:	Human Rights Committee
ICCPR:	International Covenant on Civil and Political Rights
UDHR:	Universal Declaration of Human Rights
UN:	United Nations

ABSTRACT

The rise in technological crimes like online fraud, cyberbullying, hacking, and spreading false information has posed major obstacles for Human right. This research, centered on Lideta Sub-City in Ethiopia, examines the role of the police in safeguarding human rights from breaches. The study utilized a qualitative approach, conducting in-depth interviews with 22 police officers and 15 technology-related crime victims. Thematic analysis was used to evaluate the typical offenses, their effect on human rights, and the difficulties encountered by law enforcement. Furthermore, police reports and crime records were examined as additional sources of data to support the results. The findings indicate that prevalent technology-related offenses in Lideta Sub-City consist of hacking, cyberbullying, financial fraud, and deliberately spreading fake news. Police officers recognized the increasing difficulty of these crimes due to outdated technology and inadequate cybercrime legislation. Around three-quarters of the police officers who were interviewed were team leaders, with 73% being male and having an average age of 35.6 years. Informant mentioned that the lack of proper training and resources was impeding their capability to investigate and prevent such crimes efficiently. Those who were harmed voiced worries about breaches of their privacy, freedom to speak, and safety, with certain individuals experiencing monetary damages from internet scams. This research emphasizes the pressing importance of enhancing technological capabilities, making legal reforms, and providing specialized training to empower law enforcement in protecting human rights. Additionally, it suggests utilizing a multi-stakeholder strategy that includes community education initiatives, partnering with tech professionals, and creating proactive plans to combat the increasing risk of technology-based crimes in Ethiopia. The results highlight the necessity of granting authority to law enforcement to adequately address these crimes, thus safeguarding citizens' rights in the digital era.

Key-words: Technological crime; Human rights; Police; Addis Ababa; Ethiopia

CHAPTER ONE

1. INTRODUCTION

1.1. Background of the study

Technology has become an integral part of our lives and it has revolutionized the way we live, work and communicates. However, technology has also created new opportunities for crime, and police forces around the world are facing new challenges in protecting human rights against technology-oriented crimes.

Technology-oriented crimes are any crimes that involve the use of technology, such as computers, the Internet, or mobile devices. These crimes can include:- Hacking, Cyber bullying, Identity theft, Online fraud, Child pornography, Human trafficking ,Cracking, Cyber terrorism, Cybersquatting, Creating malware, Data diddling, Data theft, Doxing, Espionage, Fake products or services, Fraud, Harvesting, Human trafficking, Identity theft, Illegal sales. Intellectual property theft, IPR violation, Phishing or vishing, Ransomware, Salami slicing, Scam-tricking, Sextortion, Slander, Software piracy, Spamming, Spoofing, Theft, Typosquatting, Unauthorized access, Vandalism, Wiretapping and others.[1]

Human rights are the basic rights and freedoms that belong to every person in the world from birth until death regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights includes the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more. Everyone is entitled to these rights without discrimination.[2]

Also In FDRE constitution it states that “Human rights and freedoms, emanating from the nature of mankind, are inviolable and inalienable”. Law enforcement officials shall at all times fulfill the duty imposed on them by law, because the state have to respect, protect and fulfill human rights in our case it is police.[3]

---

[1] Computer Hope (2023, January 10) Computer Crime.
http://www.computerhope.com/jargon/c/compcrim.htm.

[2] United Nations (1948). Universal Declaration of Human Rights.

[3] FDRE Constitution (1995). Constitution of Federal Democratic Republic of Ethiopia.

The police play a vital role in protecting human rights against technology-oriented crimes. The aim is to control and prevent crime, maintaining the peace among the public, protecting the people and the rights from the law and punishment and even the rehabilitated people also they have the skill and resources to track down perpetrators and collect evidence. So in general, it is to protect the properties and lives of the people from criminal action.[4]

This thesis paper will examine the role of police in protecting human rights against technology-oriented crime in the case of Lideta sub-city, Addis Ababa, Ethiopia. Lideta sub-city is a densely populated area of Addis Ababa, Ethiopia. It is a commercial and residential hub, and it is home to some government offices. So, it is expected to have a high rate of technology-oriented crimes.

Technology crimes have a devastating impact on the victims. They can lose money, dignity, life, sense of security. Victims of technology-oriented crimes may also suffer from emotional and psychological trauma.

1.2. Statement of the problem

Technology has become part of our daily lives, transforming the way we communicate, work, and interact with the world. However, this wide spread reliance on technology has also given rise to new forms of crime that pose significant threats to human rights. As Lideta Sub- embraces technological advancement and digitization, it is crucial to examine the role of the police in safe guarding human rights against technology-oriented crimes within this specific context.[5]

The problem at hand is the prevalence of technology-oriented crimes in Lideta sub-city and the potential violation of human rights resulting from these criminal activities.

---

[4] Haugen,Hans Morten(2012,February 1),Technology and Human Rights Friends or Foes?, Highfighting Innovations Applying to Natural Resources and Medicine, Human Rights Series No.1,William Schabas,ed.,Republic of Letters Publishing, https://ssrn.com/abstract=1991058.

[5] Yeshimar a.b, Asnake, Tadesse(2023, January 28). Analyzing Physical and Socio-economic factors for property crime incident in Addis Ababa, Ethiopia. Published online https://doi/10/0/6/j.heliyon2023

The role of the police in combating technology-oriented crimes and protecting human rights is paramount importance. However, there are several challenges that the police face in fulfilling this role effectively. These challenges may include a lack of specialized training and resources,[6] limited awareness and understanding of technology-related crimes, jurisdiction complexities and the constantly evolving nature of technological advancements. Additionally, the rapid pace of technological innovation poses difficulties for law enforcement agencies in keeping up with emerging threats and effectively investigating and prosecuting offenders.[7]

By comprehensively analyzing the existing state of technology oriented crimes, the role of the police, and the challenges they encounter, this study intends to provide valuable insights and recommendation to improve the protection of human rights within the context of Lideta Sub-city. The finding of this research will contribute to the development of more robust policies, training programs, and collaborative efforts between law enforcement agencies, technology experts, and community stakeholder to create a safer digital environment for the residents of Lideta sub-city.

1.3. Objective of the study

1.3.1. General objective

The objective of the study is to examine the role of the police in protecting human rights against technology-oriented crimes specifically within the context of Lideta sub-city.

1.3.2. Specific Objective

1. Identity and analyze the prevalent technology-oriented crimes in Lidta sub-city
2. Assess the impact of technology-oriented crimes on human right in Lideta sub-city Addis Ababa..
3. Evaluate the current role of the police in protecting human rights against technology-oriented crimes in Lideta sub-city Addis Ababa.

[6] U.S. Department of state (2023, March 20), 2022 Country Reports on Human Rights Practices:Ethiopia. https://www.state.gov/reports/2027 country-reorts-on-human-rights-practices/

[7] Unite Nations General Assembly Resolution 34/169 (1997, December 17) Code of Conduct for Law Enforcement Officials.

4. Identifying the challenges faced by the police in combating technology-oriented crimes in Lideta sub-city Addis Ababa.
5. Propose strategies and measures to enhance the role of the police in protecting human rights in in Lideta sub-city Addis Ababa.

1.4. Research Questions

1. What are the prevalent technology-oriented crimes in Lideta sub-city?
2. What are the specific human rights violations associated with these technology-oriented crimes?
3. What legal frame works or polices exist at the national and local levels to address technology-oriented crimes and protect human right in Lideta Sub-city?
4. What are the challenges faced by the police in preventing and investigating technology-oriented crimes?
5. What strategies and mechanisms do the police employ to combat technology-oriented crimes and protect human rights in Lideta Sub-city?

1.5. Significance of the study

- Addressing a gap in research: There is a lack of research in the role of police in protecting human rights against technology-oriented crimes in Ethiopia, particularly in the Lideta Sub-city. This study aims to fill this gap and provide insight into the challenge and opportunities for police in this area.
- Addressing emerging challenges: Technology-oriented crime, identity theft, and online harassment have become increasingly prevalent in the digital age. The study acknowledges the need to understand these emerging challenges and highlights the significance of the police in effectively combating such crimes while upholding human rights.
- Protecting human rights: The study recognizes that the use of technology in criminal activities can potentially infringe upon the human rights of individuals. By examining the role of the police in protecting human rights in the face of technology-oriented crimes, the study emphasizes the importance of striking a balance between law enforcement and the preservation of civil liberties.

- Enhancing law enforcement practices: Investigating the role of the police in addressing technology-oriented crimes provides insights in to their strategies, capabilities, and limitations. By identifying the challenges faced by law enforcement agencies in Lideta Sub-city, the study can contribute to the development of more effective polices and practicing in combating such crimes, ultimately leading to improve protection of human rights.[8]
- Informing policy and decision-making: The findings of the study can serve as a valuable resource for police makers, law enforcement agencies, and other stakeholders involved in combating technology-oriented crimes. The insight gained from the research can guide the formulation of evidence based polices, allocation of resources, and implementation of training programs to enhance the capacity of the police in protecting human rights within the context of technology-related offenses.
- Contributing to police reform and human rights protection: The study can contribute to police reforms and human rights protection in Ethiopia. The findings can inform the Development of policies and practices that promote human rights protection in law enforcement, particularly in the Federal Police crime investigation bureau. Overall, the significance of the study lies in its exploration of the role of the police in protecting human rights against technology-oriented crime in Lideta sub-city. It raises awareness about the challenges, opportunities, and a potential solution in this domain, aiming to contribute to the advancement of polices practices, and academic discourse surrounding the intersection of law enforcement, technology, and human rights.

1.6. Scope of the study

The study focuses on the role of police in Lideta Sub-city is a specific geographic area, and the research will be limited to this particular location. It does not encompass other Sub-city, city or regions.

[8] Wario Elemo(2020,June).Police Reform and Human Rights Protection in Ethiopia:The case of Federal PoliceCrimeInvestigationBureau.p7 .http://etd.aau.edu.et/bitstream/handle/123456789/22277/Wario%20Elemo%20Final%20Thesis%20paper.pdf?sequence=1&isAllowed=y

1.7. Limitation of the study

The research offers a number of important contributions, but it does have its shortcomings that are worth mentioning. First of all, the study is geographically limited to Lideta Sub-city of Addis Ababa City. Moreover, it narrows down the activities of crime only to technology related crimes; the other aspects of criminal behaviors would be covered by other studies. The investigation will focus on the role of police as the defender of human rights without giving due attention to other actors of Human Rights. In addition, the study will not employ historical analysis as a method but would only describe the rampant technology related crimes as a new phenomenon and shows how pressing it has becoming.

1.8. Ethical considerations

Ensure that ethical considerations are addressed throughout the research process. Due to the sensitive nature of the study, especially involving crime victims, ethical considerations are crucial. Participants were fully informed about the study's purpose and their rights, and informed consent was obtained. The participants were allowed to withdraw at any time without consequences. To protect privacy, all personal data was anonymized, with pseudonyms used in reports. The researcher handled the interview process carefully to minimize harm, particularly for victims recalling traumatic events. Ethical approval from an institutional review board was also secured to ensure compliance with research standards and participant welfare.

1.9. Research methodology

1.9.1. Research approach and design

This study employed a qualitative research approach, which is appropriate given the focus on understanding personal experiences, and perceptions. Qualitative research allows the exploration of complex phenomena through rich, descriptive data, making it well-suited for

studying the role of the police in protecting human rights in the context of technology-oriented crimes[9].

The research design is exploratory was used. The study is structured around semi-structured interviews as the primary data collection tool, which allows flexibility in exploring individual perspectives[10]. The interviews will be complemented by an analysis of secondary data such as reports, documents, and police records related to technology-oriented crimes. The research design is particularly suited to understanding social constructs and interpreting the complex interplay between police actions and human rights in the face of evolving technology-based crimes. The study will utilize interpretive analysis to identify patterns, themes, and meanings in the data, allowing the researcher to uncover insights into the effectiveness of police interventions and their impact on human rights. The research design also incorporated the review of secondary documents, which adds a layer of context and supports the primary data

1.9.2. Sampling methods, size and population

A purposive sampling technique has been chosen for this study due to its effectiveness in selecting participants who are directly relevant to the research topic[11]. The researcher intentionally selects individuals who possess unique knowledge or experiences related to technology-oriented crimes, ensuring the collection of rich and insightful data. The police officers included in the study were those who have dealt with technology-related crimes and human rights protection within Lideta sub-city, providing expert perspectives on their role in addressing these crimes. Similarly, victims of these crimes were selected based on their direct experience with offenses such as online fraud, cyberbullying, and identity theft.

The sample size of 37 participants (22 police officers and 15 victims) were included and considered sufficient for the study, as qualitative research values depth of insight over breadth

[9] Creswell, J. W., & Poth, C. N. (2017). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.

[10] ibid

[11] Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed-method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), 533-544.

of representation. However, the sample size for the study was determined by the principle of saturation, in which data collection was stopped when the idea was repeated and no more new responses had not been generated by the participants.

1.9.3. Data types and sources

The data collection for this study involved gathering information from both primary and secondary sources. The researcher conducts in-depth interviews as a primary data collection method. Additionally, secondary data sources were utilized, such as annual crime reports and property crime records obtained from Lideta Sub-city police officers. These secondary data sources will be employed for crime mapping and analysis purposes.

1.9.4. Methods/techniques/ instruments of data collection

1.9.4.1. In-depth interview

The primary tool for data collection in this study is the semi-structured interview, chosen for its flexibility and ability to gather in-depth insights from participants. Semi-structured interviews provide a structured yet open framework, allowing participants to share their experiences while giving the researcher the ability to probe further into specific areas of interest[12]. Therefore, police officers and team leaders were interviewed about their experiences in investigating technology-related crimes, their strategies for human rights protection, and any challenges they have faced in their work. Victims were asked to reflect on their experiences with these crimes and their interactions with law enforcement. Each interview is expected to last between 30 to 60 minutes, and all interviews were recorded (with the participants' consent) to ensure accuracy during transcription and analysis.

1.9.4.2. Document review

In addition to interviews, the study was also relying on secondary data collection through document analysis. Relevant reports, official records, and legal documents related to technology-oriented crimes and human rights violations were reviewed. These documents

[12] Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. British Dental Journal, 204(6), 291-295.

provide supplementary data that helps contextualize the interview findings, offering a more holistic understanding of the research topic.

The researcher had been reviewing relevant documents; the document review can involve examining various types of documents relevant to the topic. The specific documents that can be reviewed include:

1. Police Reports: Analyzing police reports related to technology-oriented crimes in Lideta sub-city can provide insights into the nature and extent of these crimes. It can help identify trends, patterns, and specific cases that highlight the challenges faced by the police in addressing such crimes while protecting human rights.
2. Legal Frameworks: Reviewing relevant laws, regulations, and policies related to technology-oriented crimes and human rights protection is crucial. This includes national laws, international conventions, and local ordinances that guide the police's actions and responsibilities in dealing with technology-oriented crimes. Understanding the legal framework helps assess the adequacy of existing provisions and identify any gaps or areas for improvement.
3. Police Manuals and Guidelines: Examining police manuals, operational guidelines, and standard operating procedures specific to technology-oriented crimes can shed light on the strategies, protocols, and best practices employed by the police in Lideta sub-city. These documents outline the recommended procedures for investigating, preventing, and responding to technology-oriented crimes while ensuring the protection of human rights.
4. Policy Documents: Analyzing policy documents related to technology-oriented crime and human rights at the local, regional, or national level can provide insights into the broader context in which the police operate. These documents may include strategies, action plans, or policy statements that outline the goals, objectives, and priorities for addressing technology-oriented crimes while upholding human rights

1.9.5. Method of data analysis

The data collected through interviews and documents was analyzed using thematic analysis, a widely used method in qualitative research. Thematic analysis involves identifying, analyzing, and reporting patterns or themes within the data, which allows the researcher to make sense of

large amounts of qualitative information. The process begun with transcription of the interview recordings, ensuring that all participant responses are accurately documented. The researcher then engaged in familiarization with the data by reading through the transcripts and document notes, allowing key ideas and patterns to emerge. After this, the researcher proceeded with coding, a systematic process where key segments of data were labeled with descriptive tags or "codes" that highlight important information[13]. These codes were then be grouped into broader themes that reflect the core issues discussed by participants, such as the challenges of policing technology-oriented crimes, the effectiveness of human rights protection, and the experiences of crime victims.

Once the themes have been identified, the researcher was interpreted the data in relation to the study's research questions, using the participants' narratives to provide insights into the police's role in addressing these crimes. The secondary data collected from documents was also be analyzed thematically, helping to provide a comprehensive understanding of the issue by linking the interview findings with broader trends and policies related to technology-oriented crimes and human rights.

1.10. Organization of the study

The thesis is organized into several key chapters that systematically address the research objectives. The first chapter provides an introduction to the study, outlining the background, research problem, objectives, and significance of the research Chapter Two reviews relevant literature on technology-oriented crimes and their impact on human rights, along with the associated framework. Chapter three presents the result, findings from in-depth interviews and discussions. Finally, chapter four offers conclusions and recommendations, proposing strategies to enhance the police's capacity to combat technology-oriented crimes.

[13] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

CHAPTER TWO

2. LITERATURE REVIEW:

2.1. Introduction

Technological advancement is transforming societies worldwide and giving rise to a new wave of criminal activities known as technology-driven crimes or cybercrimes. Law enforcement agencies globally, including in Ethiopia, face major challenges from crimes that exploit vulnerability in digital infrastructure. As technology becomes more intertwined with daily life, safeguarding human rights from the dangers associated with these offenses has become a key focus for law enforcement. This review delves into technology-focused crimes, their relationship with human rights, the struggles Ethiopian police encounter in combating them, and ways to strengthen police efforts in protecting human rights from these threats.

2.2. Technology and concepts of Technology-Oriented Crimes

Technology involves utilizing scientific knowledge to develop machines, systems, and devices that improve human abilities and address issues. As technology advances, it spreads into all areas of life, including communication, education, commerce, and governance. Yet, technology has also led to the rise of technology-oriented crimes, like hacking, identity theft, online fraud, and cyberstalking, in addition to its advantages[14]. Public agencies are increasingly required to innovate quickly as technology is now widespread in society and constantly advancing. Technology has played a crucial role in police work, and the advancement of technology has progressed alongside the changes in police procedures.[15]

Technology-oriented crimes refer to crimes focused on technology using computers, digital devices, and the internet to commit illegal activities. These crimes can cause extensive financial, psychological, and social damage by targeting individuals, businesses, governments,

[14] Dron, J. (2022). Educational technology: what it is and how it works. AI & SOCIETY, 37(1), 155-166.

[15] Nielsen, J., & Keasling, J. D. (2016). Engineering cellular metabolism. Cell, 164(6), 1185-1197.

or institutions. Technology-based crimes are characterized by their dependence on digital infrastructure like the internet, computers, and mobile devices to carry out illicit activities.[16,17] The definition of cybercrime has broadened as technology has progressed, moving beyond basic acts like hacking to more intricate criminal activities like identity theft, cyber espionage, and data breaches[18]. Technology-related crimes can be divided into two main categories: crimes where technology is used as the main method for committing the crime and crimes where technology is the focus of the crime[19].

In cases involving technology as the main tool, criminals use the internet and other digital platforms for activities like phishing, online fraud, and spreading malware. On the other hand, in offenses targeting technology, perpetrators aim to harm or cause chaos in digital systems, as evidenced by hacking, data breaches, and cyberattacks on government or corporate networks[20]. Technology-related crimes frequently cross international boundaries, posing difficulties for local law enforcement agencies in effectively addressing them. The internet's worldwide reach allows cybercriminals to commit crimes in one country while focusing on victims in another, making the prosecution of these offenses more challenging[21].

[16] Demetis, D. (2023). Organised crime-the cyber dimension. A Research Agenda for Organised Crime, 177-194.

[17] Kovacich, G. L., & Boni, W. C. (2011). High-technology crime investigator's handbook: Establishing and managing a high-technology crime prevention program. Elsevier.

[18] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.

[19] McGuire, M. R. (2022). Crime, Control and the Ambiguous Gifts of Digital Technology. *The SAGE Handbook of Digital Society*, 35.

[20] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.

[21] Rutenberg, I., & Sugow, A. (2020). Regulation of the Social Media in Electoral Democracies: A Case of Kenya. *SOAS LJ*, *7*, 301.

2.3. Types of Technology-Oriented Crimes

Technology-oriented crimes encompass a wide range of offenses that exploit digital technologies and online platforms. In the types of technology-oriented crimes commonly encountered include:

1. Hacking and Unauthorized Access: Hacking involves illegally accessing computer systems or networks to steal, alter, or delete data. Hacking can result in the exposure of confidential data and put the privacy of individuals and organizations at risk. In Ethiopia, the number of hacking incidents is on the rise as more industries shift to digital operations. This form of criminal activity frequently entails taking advantage of software or network weaknesses to access confidential systems. Hackers might focus on individuals, corporations, or governmental agencies. Ransomware is one of the most well-known types of hacking, involving hackers blocking users' access to their systems or data until a payment is made. Cybercriminals can also commit data breaches, in which they steal and potentially sell sensitive information like personal, financial, or proprietary data on the dark web or for other harmful intentions.[22].

2. Phishing and Identity Theft: Phishing is when someone pretends to be a trustworthy source in order to trick people into giving up personal information like passwords or credit card numbers using emails or fake websites. Identity theft happens when thieves use stolen personal information to pretend to be another person, usually to make money. The increasing internet usage in Africa has exposed the population to these scams Phishing is a type of online scam in which criminals try to deceive people into sharing personal information, like passwords, credit card numbers, or social security details. Phishing attacks frequently come in the guise of misleading emails, messages, or websites that pretend to be legitimate organizations or individuals. These deceptive messages usually pressure the recipient to act quickly, like clicking a link or sharing personal details.[23].

[22] Smith, L., Chowdhury, M. M., & Latif, S. (2022). Ethical hacking: Skills to fight cybersecurity threats. EPiC Series in Computing, 82(5), 102-111.

[23] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

When criminals successfully gather personal information through phishing or other means, they may commit identity theft, using the victim's identity to conduct illegal activities such as opening bank accounts, taking out loans, or making unauthorized purchases. Identity theft can cause significant financial damage and emotional distress for victims[24].

3. Online Fraud and Scams: Various types of deceit carried out on the internet, such as counterfeit e-commerce websites, investment scams, and online pyramid schemes, fall under the umbrella of online fraud. Many times, these scams focus on users who are not aware and lead to big financial losses. The main types of online fraud include the following activities:

Online shopping fraud: Scam websites or fake listings on real e-commerce sites trick consumers into purchasing items or services that they never receive.

Investment scam: Culprits entice individuals with fake investment chances, frequently guaranteeing impressive profits, but ultimately abscond with the capital invested. Instances like Ponzi schemes and frauds within the realm of cryptocurrency are illustrative.

Auction fraud involves scammers on auction sites selling items that are either fake or don't actually exist, deceiving buyers into purchasing goods that are not as valuable as claimed. Online fraud victims may face substantial financial losses, and the anonymity of the internet can make it challenging to investigate and prosecute these crimes.

4. Cyberbullying and Harassment: Cyberbullying refers to the utilization of online communication tools to bully, scare, or shame people, which can result in emotional and mental damage. Cyberbullying in Ethiopia has impacted vulnerable groups like children and women, threatening their mental well-being and dignity. Cyberstalking is the use of digital technologies to harass, intimidate, or stalk individuals. It may involve sending intimidating messages, monitoring someone's internet actions, or spreading harmful gossip about the person. Cyberstalking can happen via email, social media, messaging apps, or by gaining unauthorized access to a victim's devices [25].

[24] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

[25] Saleem, S., Khan, N. F., Zafar, S., & Raza, N. (2022). Systematic literature reviews in cyberbullying/cyber harassment: A tertiary study. Technology in Society, 70, 102055.

Cyberbullying is a particular type of online abuse in which individuals, frequently young people, are exposed to continual and focused mistreatment, rude remarks, or embarrassment via internet platforms. This may lead to serious psychological consequences, such as anxiety, depression, and, in severe situations, suicide. Both cyberstalking and cyberbullying violate the victims' safety rights and can cause lasting emotional and psychological harm. Regrettably, individuals who commit these offenses frequently take advantage of the internet's anonymity, leading to challenges in identifying and holding them accountable.[26]

5. Dissemination of Hate Speech and Disinformation: The rise of social media platforms has contributed to escalating ethnic and political tensions in Ethiopia by enabling the spread of hate speech and false information. These actions often lead to unrest in society and could infringe upon individuals' rights to peace and security[27]. The widespread use of social media and various online platforms has resulted in the rapid dissemination of hate speech, misinformation, and false information. Promoting hate speech involves spreading messages that encourage violence, discrimination, or hostility towards individuals based on their race, religion, ethnicity, gender, or sexual orientation.

The intentional dissemination of false information, also known as disinformation, can result in significant impacts, especially when it is used to sway public opinion, elections, or geopolitical conflicts. False information and misinformation schemes are frequently planned by people, organizations, or even government officials aiming to distort reality for self-interests, political motives, or financial benefits. These types of content on the internet have the potential to worsen social conflicts, encourage violence, and weaken democratic systems, posing a major worry for governments and law enforcement organizations around the globe[28].

---

[26] Larrañaga, M. G., Iglesias, E. J., & Aizpuru, N. L. (2023). Bullying and cyberbullying: Victimisation, harassment, and harm. The need to intervene in the educational centre. Revista Española de Pedagogía, 77(273), 14.

[27]Prahassacitta, V., & Harkrisnowo, H. (2021). Criminal disinformation in relation to the freedom of expression in Indonesia: A critical study. Comparative Law Review, 27, 135-165.

[28] Brüggemann, S., Kutlu, N., Müller-Török, R., Prosser, A., Ručinská, S., Szádeczky, T., & Vrabie, C. (2022). A scientific basis for a policy fighting fake news and hate speech. OCG/Facultas, 101.

2.4. Understanding Technology-Oriented crimes and their implication on Human Right

Crimes related to technology have significant effects on human rights, especially in areas like privacy, freedom of speech, security, and information accessibility. These offenses can violate various basic rights protected by Ethiopian law and global human rights agreements like the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR)[29].

Crimes related to technology have important effects on human rights. Human rights, according to international groups such as the United Nations, include the rights to privacy, freedom of speech, and safeguard against discrimination. Crimes related to technology have the potential to infringe upon these rights, either through direct or indirect means. Hacking personal or corporate data violates the right to privacy, whereas cyberbullying and hate speech infringe on the rights to dignity and freedom from discrimination.[30]. Furthermore, the distortion of information via deepfakes and false news impacts the freedom of expression and availability of truthful information. As technology progresses, it is becoming more and more crucial to safeguard human rights from violations caused by technology.

Advancements in technology also make it easier for surveillance activities to impinge on individual rights, especially in terms of privacy. Governments and corporations frequently utilize sophisticated technological resources to observe citizens, gather personal information, and monitor online behaviors. Although these tools can be used for security, they can also be abused, resulting in infringements on the right to privacy and personal freedom. This debate over security and privacy highlights the importance of having laws that weigh the advantages of technology against safeguarding human rights[31].

The right to privacy is one of the most important human rights issues connected to technology-related crimes. Unauthorized access to personal information in activities such as

[29] ibid

[30] ibid

[31] ibid

hacking, phishing, and identity theft can result in privacy violations for individuals. The African Union Convention stresses the significance of protecting personal data in the digital era, but numerous Ethiopians still face privacy risks because of inadequate cybersecurity measures.[32]

Cyberbullying, harassment on the internet, and sharing unauthorized images can violate people's dignity and integrity. Individuals, especially women and children, who are targeted in these crimes, frequently suffer from enduring emotional and psychological distress. Law enforcement agencies in Ethiopia have a vital role to play in safeguarding individuals from technology-oriented crimes due to their extensive human rights implications. Nevertheless, law enforcement encounters multiple obstacles when trying to effectively address these crimes[33].

2.5. Objectives of Human Rights Protection from Technology-Oriented Crimes

The main goal of safeguarding human rights in relation to technology-related offenses is to prevent technological progress from violating people's basic rights. This involves a holistic strategy that covers preventing, detecting, and prosecuting technology-related crimes while ensuring privacy, freedom of speech, and other human rights are protected. In the digital age, safeguarding human rights requires establishing a legal structure to ensure accountability for wrongdoers and to prevent excessive use of power by governments or corporations under the guise of security.[34]

A key objective of human rights protection in this area is to make sure that law enforcement agencies have the appropriate tools and training to address technology-related crimes without violating individual rights. Furthermore, global collaboration is essential, since cybercriminals

[32] Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. Journal of Big Data, 11(1), 118.

[33] Ibid

[34] Nosál, J. (2023). Crime in the Digital Age: A New Frontier. In The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network (pp. 177-193). Cham: Springer International Publishing.

frequently work across boundaries, aiming for victims in various nations. Hence, it is crucial to establish global legal guidelines that support responsibility, openness, and the safeguarding of human rights in order to combat technology-related crimes efficiently.[35].

2.6. The Evolving Landscape of Technology-Oriented Crime: Trends and Challenges

The landscape of technology-driven crime is always shifting as offenders discover new ways to profit from advancements in technology. The rise of complex malware, cryptocurrencies, and the dark web, online hate speech and disinformation has presented new challenges for law enforcement organizations in their hunt for, investigation of, and conviction of criminals. When criminals utilize these technologies to be anonymous, it becomes more difficult to find and prosecute them, especially if they are not in the same nation as their victims. Furthermore, because technology is advancing so quickly, many law enforcement agencies lack the necessary tools to deal with the growing complexity of crimes involving technology[36].

A notable trend in technology-related crime is the growing prevalence of social engineering tactics, in which criminals coerce people into revealing sensitive data. This pattern highlights the importance of increased understanding and education on online security practices. Moreover, the increase in ransomware attacks, in which cybercriminals prevent victims from accessing their systems or data until a ransom is given, is a major worry for individuals, businesses, and governments.[37]

2.7. The Role of Police and Law Enforcement Agencies in Promoting and Protecting Human Rights against Technology-Oriented Crimes

Law enforcement agencies play a pivotal role when it comes to fighting crimes involving technology; law enforcement organizations play a critical role in promoting and defending human rights. Their responsibilities include investigating cybercrimes, catching offenders, and

[35] ibid

[36] Demetis, D. (2023). Organised crime-the cyber dimension. A Research Agenda for Organised Crime, 177-194.

[37] ibid

ensuring that victims' rights are upheld throughout the judicial process. However, while pursuing these objectives, law enforcement agencies must ensure that their actions do not infringe upon people's rights, such as freedom of speech and privacy.[38]

Law enforcement personnel need to be highly skilled in data analysis, digital forensics, and cybersecurity since technology-related crimes are complex. More and more police agencies across the globe are establishing specialized cybercrime sections to deal with these particular offences. However, the global reach of cybercrime, inadequate funding, and inadequate training provide serious difficulties for law enforcement organizations, particularly in underdeveloped nations.[39]

Furthermore, the possibility of human rights violations is becoming increasingly apparent as law enforcement relies more on technology to combat crimes involving technology. Surveillance tools meant for combating cybercrime can be easily exploited, resulting in privacy abuses and infringement of civil liberties.[40]. Therefore, it is imperative that law enforcement agencies, including the police, operate under a robust legislative framework that places a premium on accountability.

For law enforcement officers, training and capacity building are essential investments. In order to investigate and combat cybercrimes, police personnel must possess the requisite knowledge and abilities. Digital forensics, cyber investigative techniques, and the use of specialized software to track down online criminal activity are among the subjects that must be studied for this. In order to prevent breaching people's rights to privacy, freedom of speech, and access to information while combating cybercrime, law enforcement officials should receive training in human rights principles in addition to technological abilities. It is possible to improve training programs and fortify Ethiopian law enforcement's skills by working with

[38] Jimma, E. (2022). College of Law and Governance School of Law LLM in Human Rights and Criminal Law (Doctoral dissertation, Jimma University).

[39] ibid

[40] ibid

international organizations and cyber security experts[41]. Ethiopia's legislative structure needs to be strengthened in order to effectively combat technology-related crimes and address emerging issues in cybersecurity and data protection. This entails updating the legislation to reflect new forms of cybercrime and ensuring that law enforcement has the means to find and prosecute offenders[42].

Moreover, international cooperation is necessary to combat technology-related crimes that cross national borders. To facilitate information sharing, coordinate investigations, and develop cohesive strategies for combating cybercrime, Ethiopian law enforcement agencies must work with foreign law enforcement agencies, the African Union, and international organizations such as INTERPOL[43].

It is crucial to educate the public about the dangers of technology-related crimes in order to prevent individuals from becoming victims and to promote collaboration with law enforcement agencies. Public awareness campaigns aim to educate both individuals and organizations on the importance of safeguarding themselves online through practices like strong password usage, avoiding phishing scams, and securing sensitive data[44].

Awareness campaigns should place a high priority on encouraging victims of cybercrime to report events to law enforcement in addition to prevention efforts. Building public and law enforcement trust is crucial to enhancing cooperation and bolstering the police's ability to look into and stop cybercrime. While monitoring plays a crucial role in stopping cybercrime, it must be done so in a way that respects people's civil rights and privacy. Law enforcement agencies must set up clear guidelines for the use of surveillance technology and ensure that

[41] ibid

[42] ibid

[43] ibid

[44] ibid

they are only used when it is truly necessary to prevent criminal activity. Mechanisms should also be in place to supervise the use of surveillance equipment and stop any abuse[45].

2.8. Policing Models and Practices: International Perspectives on Protecting Human Rights

International policing of technology-related crimes demonstrates common themes, including the need for specialized cybercrime units, international cooperation, and the use of technology to combat crime while protecting human rights. The rise in technology-related crimes in Kenya has prompted the government to enact laws such as the Computer Misuse and Cybercrimes Act of 2018, which creates a framework for investigating and prosecuting cyber offenses while protecting people's rights to privacy[46]. Kenya's law enforcement agencies have established cybercrime units to combat digital crimes, but challenges remain in terms of resource allocation and technical expertise[47].

South Africa has faced challenges regarding fighting technology-related crimes has presented significant challenges for South Africa, particularly in the areas of online fraud and hacking. The South African government has put the Cybercrimes Act of 2020 into effect in order to combat cybercrime and protect people's rights. However, a lack of funding has made it difficult for authorities to adequately investigate and imprison those who violate the legislation, which has hampered the execution of this rule[48].

The United States has one of the most advanced frameworks for combating technology-oriented crimes. When it comes to dealing with offenses using technology, the US has one of the most advanced systems. With the use of statutes like the CFAA and the ECPA, the FBI

[45] Niezen, R. (2020). Human Rights: The Technologies and Politics of Justice Claims in Practice. Stanford University Press.

[46] Otele, O. (2021). Kenya's data protection regime: challenges and future prospects. journal of African politics, 1(1), 66-88.

[47] Aineah, A. (2022). News processes, opportunities and challenges in converged Kenyan newsrooms: a case study of Standard Group Plc.

[48] Omidosu, J. (2023). A social-technical harm-based taxonomy of online hate in South Africa.

and DHS look into cybercrimes. Though they offer robust protections for human rights, concerns about the potential overreach of government monitoring programs and the necessity of striking a balance still exist[49]. While these frameworks offer robust protections for human rights, concerns remain about the potential overreach of government surveillance programs and the need to balance national security with individual privacy[50]

Germany is known for its strong emphasis on defending individual rights to privacy, which is further strengthened by the General Data Protection Regulation (GDPR). To combat crimes centered on technology while preserving individual rights, the German government established specialized teams to combat cybercrime. Germany is renowned for having some of the most sophisticated cybercrime prevention methods in the world, yet law enforcement continues to face challenges due to the rapid advancements in technology[51].

2.9. The Role of Ethiopian Police in Protecting Human Rights

Ethiopia has come a long way in creating laws to combat crimes involving technology, particularly since the 2016 Computer Crime Proclamation went into effect. This act creates a framework to protect human rights online by outlawing identity theft, hacking, and the dissemination of false information. However, Ethiopia faces challenges in enforcing these regulations due to inadequate resources and poor technical competence.[52].

When it comes to defending human rights in situations when offenses using technology are involved, Ethiopian law enforcement is essential. However, like many other developing countries, Ethiopia struggles to improve the technological capacities of its law enforcement authorities so that cybercrimes may be effectively investigated and prosecuted. To effectively

[49] Demetis, D. (2023). Organized crime-the cyber dimension. A Research Agenda for Organized Crime, 177-194.

[50] Thomas, K. V. (2021). The Role of Science & Technology in Law–Enforcement. The Indian Police Journal, 35.

[51] Trierweiler, M. K. (2021). Development of an IT-supported anti-fraud-framework for SMEs: An architectural concept for risk management using the'Man-Technology-Organization ‘approach. In STPIS (pp. 204-215).

[52] Zeynu, H. J. (2022). Human Rights Focused Regional Police Reform Guidance in Ethiopia. Hawassa UJL, 6, 130.

combat technology-related crimes and protect the public, law enforcement must have the right equipment and training[53].

The role of Ethiopia's police force is to investigate crimes, put an end to illicit activities, and apprehend those who commit them, just like the police forces of other nations. These obligations have expanded in the current digital age to include offenses connected to technology, such as identity theft, cyber fraud, hacking, and online harassment. Human rights may be severely violated by these violations, particularly in cases when someone are subjected to online harassment and intimidation or when personal information is collected unlawfully. Law enforcement is therefore essential to ensuring that those who commit these crimes are held accountable and that victims are protected from further harm[54].

A primary challenge faced by Ethiopian law enforcement in this regard is the lack of adequate technical expertise and resources to effectively address crimes involving technology. The police have attempted to establish cybercrime divisions, but these teams often lack the resources and expertise needed to stay up to date with the rapidly evolving world of cybercrime. As a result, law enforcement is less able to protect human rights in the digital sphere[55].

Concerns have also been raised about the potential for Ethiopian law enforcement forces to abuse their power, particularly when it comes to population monitoring. Police agencies are relying more and more on technology to investigate cybercrimes, but there is a risk of abuse that could breach people's rights and privacy. This highlights how crucial it is to have strong

[53] Yilma, K. M. (2021). Cybercrime Lawmaking and Human Rights in Ethiopia. Mizan Law Review, 15(1), 73-106.

[54] Ayalew, Y. E. (2020). Assessing the limitations to freedom of expression on the internet in Ethiopia against the African Charter on Human and Peoples' Rights. African Human Rights Law Journal, 20(1), 315-345.

[55] ibid

legal frameworks and oversight procedures in place to guarantee that law enforcement officials carry out their duties while respecting human rights[56]

In addition to these difficulties, the Ethiopian police also have coordination issues with other organizations and parties involved in the fight against crimes centered on technology. Because cybercrime is so commonplace worldwide, effective collaboration with foreign law enforcement organizations is essential. However, the poor technical infrastructure and skill of the Ethiopian police force has hindered their ability to effectively engage in this cooperation. To meet these obstacles and guarantee that Ethiopian police can effectively protect human rights in the contemporary era, significant funding for technology, training, and legislative changes will be needed[57].

2.10. Legal Frameworks and Human Rights Standards for Policing Technology-Oriented Crimes in Ethiopia

Ethiopia has revised its laws about crimes involving technology by enacting new laws that aim to criminalize various forms of cybercrime. The significance of the Computer Crime Proclamation No. 958/2016 lies in the establishment of the legal foundation for the prosecution of persons involved in technology-related crimes, including identity theft, cyber fraud, and hacking[58]. This statement was a big step toward recognizing the threat posed by cybercrime and the need for laws to be put in place to combat it.[59]. This proclamation was a significant step forward in recognizing the threat posed by cybercrime and the need for legal tools to address it.

The Computer Crime Proclamation enumerates a number of offenses related to digital networks and computers, including online fraud, the dissemination of malicious software, and

[56] Abaje, O. (2024). Cybercrime Threats and Trends in Ethiopia: Critical Legal Analysis. Wallaga University Journal of Law, 1(2), 18-33.

[57] Mehari, S. A. Implications of the Ethiopian Computer Crime Proclamation on the Enjoyment of Human Rights.

[58] Yilma, K. M. (2021). Cybercrime Lawmaking and Human Rights in Ethiopia. Mizan Law Review, 15(1), 73-106.

[59] ibid

illegal system access. In order to protect people's privacy, the legislation also forbids the unlawful gathering of personal information and the recording of conversations.[60].

Nevertheless, despite offering a strong basis for tackling cybercrime, the Computer Crime Proclamation has shortcomings in its enforcement, specifically in safeguarding human rights. A critical concern is the requirement for increased legislation that deals with new types of technology-focused crimes like cyberbullying, online harassment, and digital surveillance. These offenses frequently impact the human rights of victims directly, such as their entitlement to respect, confidentiality, and being free from prejudice. As technology advances, it is necessary to revise the legal system to combat emerging cybercrimes without infringing upon human rights additionally; more clarity and transparency are required in enforcing laws concerning technology-focused offenses in Ethiopia. Despite the extensive authority given to law enforcement by the Computer Crime Proclamation, there are fears that these powers may be abused, resulting in human rights violations. One instance of this is when law enforcement is given the power to monitor communications and search computer systems without sufficient protections against misuse[61]. This highlights the need for clear rules and monitoring measures to ensure that police activities conform to human rights norms.

Along with its national laws, Ethiopia has also agreed to various global agreements and treaties that set out human rights guidelines for crimes related to technology. These consist of the UDHR, ICCPR, and the African Charter on Human and Peoples' Rights[62]. These global agreements offer a wide-ranging structure for safeguarding rights like privacy, freedom of speech, and protection against discrimination in the digital era.

The lack of resources and technical expertise within law enforcement agencies in Ethiopia makes it even more challenging to implement international human rights standards in policing technology-oriented crimes. Despite Ethiopia showing a strong dedication to international human rights agreements, the police struggle to effectively enforce cybercrime standards

[60] ibid

[61] Nebiat, L. (2017). The Legal and Institutional Framework for the Corporate Governance of State-Owned Enterprises in Ethiopia (Doctoral dissertation).

[62] Smith, R. K. (2022). International human rights law. Oxford University Press.

which lead to challenges in investigating and prosecuting such offenses[63]. Dealing with this problem will involve the need for capacity-building initiatives, such as providing training for law enforcement personnel on the technical aspects of cybercrime and the human rights consequences of their behaviors[64].

CHAPTER THREE

3. RESULT AND DISCUSSION

3.1. Introduction

The results of the study, which examined how police in Lideta sub-city protect human rights against crimes involving technology, are presented in this section. In-depth interviews with 22 police officers and 15 victims yielded data, which was then analyzed using thematic analysis to identify trends and themes. The study was further enhanced by the inclusion of secondary data. The aim of study aligns with the stated primary themes and subthemes. Direct quotes from the participants support each topic, which is then followed by an analysis of the results and a discussion of their significance for the defense of human rights and law enforcement in cases of technology-driven crime.

3.2. Personal characteristics

The study involved 37 participants, 15 of whom were victims and 22 police officers, chosen for the study using the saturation approach. Seventy-five percent of the police officers, who were on average 35.6 years old, were in leadership roles. The police participants were predominantly male (73%) with an average tenure of 17 years on the force. Remarkably, very few police personnel had any training on crimes involving technology. In contrast, the victims were 53% male and had an average age of 31.4 years.

[63] Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. Commonwealth Law Bulletin, 46(1), 78-109.

[64] ibid

3.3. Prevalence and Types of Technology-Oriented Crimes

The study identified various types of technology-oriented crimes prevalent in Lideta sub-city, including cyberbullying, online fraud, hacking, and the dissemination of harmful or illegal content. Among the police officers interviewed, more than two-thirds acknowledged that the dissemination of hate speech and disinformation, mobile banking fraud, and social media-related insults were common crimes they encountered. The following are common types of technological crime described during interviews.

3.3.1. Dissemination of hate speech and disinformation

The increase of hateful speech and false information on social media platforms in Ethiopia has significantly contributed to the rise of political and ethnic tensions. The spread of hateful content on social media, which promotes violence and animosity, violates people's rights to peace and security. One police officer highlighted,

> *"False information and hate speech are on the rise, escalating societal discontent and adding to the workload of law enforcement" (A female police officer, 35 years of age)*).

Hate speech often targets individuals based on ethnicity, religion, or gender, with the intent to incite violence or discrimination. Disinformation, on the other hand, is intentionally misleading and is used to manipulate public opinion, destabilize elections, or fuel geopolitical conflicts.

The rapid spread of false information and hate speech poses a serious threat to social harmony and democracy. Disinformation campaigns can distort reality, inflame social divisions, and threaten national stability, creating a challenge for law enforcement to control and mitigate the damage. As observed globally, governments and law enforcement agencies struggle to keep pace with the evolving tactics used in online hate speech and disinformation[65]. Combatting

[65] ibid

this requires a collaborative effort involving updated laws, social media regulations, and public awareness campaigns to limit the spread of such harmful content[66].

3.3.2. Financial frauds, Online Fraud and Scams

Participants reported that mobile banking-related crimes, sites selling items that are either fake or don't actually exist, deceiving buyers into purchasing goods that are not as valuable as claimed were particularly prevalent in the area. One police officer, a team leader with 17 years of experience, noted,

> *"Mobile banking related crimes and insults on social media are common types of crime in my perception"* (Male police team leader, 38 years old).

Another officer highlighted hacking and financial fraud as significant issues, alongside cyberbullying, stating,

> *"Financial frauds are common types of crimes in Ethiopia, especially fraud related with mobile banking'' (*Female police officer, 32 years old).

Moreover, scammers on auction sites selling items that are either fake or don't actually exist; deceiving buyers into purchasing goods that are not as valuable as claimed. Online fraud victims may face substantial financial losses, and the anonymity of the internet can make it challenging to investigate and prosecute these crimes[67].

> *"I had no idea about technological crime until I lost money through an online shopping*" (Female victim, 26 years old).

This illustrates how financial fraud not only affects individuals financially but also demonstrates a lack of awareness among the general population about technology-related crimes. Therefore, the current report suggests that technology-oriented crimes are becoming increasingly prevalent in Lideta sub-city. This is consistent with global trends, as other studies

[66] Santuraki, S. U. (2019). Trends in the regulation of hate speech and fake news: a threat to free speech?.Hasanuddin Law Review, 5(2), 140-158.
[67] Cross, C. (2019). Online fraud. Oxford research encyclopedia of criminology, 1-32.

have found similar patterns in urban areas where access to technology is rapidly expanding[68]. Financial fraud and cyberbullying are particularly troubling, as they target vulnerable individuals who may lack the digital literacy needed to protect themselves. These findings highlight the need for enhanced community education and better legal frameworks to address such crimes[69].

3.3.3. Cyberbullying

Several participants also highlighted the impact of cyberbullying it is very common to harass, threaten, embarrass, or target another person through social medias. A victim of cyberbullying, noted,

> *"The technological crime affects my right to freedom of speech, as I was bullied for expressing my opinion online."* (Male victim,45 years old)

This suggests that cyberbullying is not only a social issue but also has implications for human rights, particularly the freedom of expression. The prevalence of cyberbullying in Lideta Sub-City indicates a growing challenge for law enforcement. Given the limited resources and knowledge among the police, there is a need for more focused training and the development of robust legal frameworks to address these crimes. The report is consistent with another study that reported cyberbullying is a particular type of online abuse in which individuals, frequently young people, are exposed to continual and focused mistreatment, rude remarks, or embarrassment via internet platforms[70]. This may lead to serious psychological consequences, such as anxiety, depression, and, in severe situations, suicide[71]. The study also highlights the importance of public awareness initiatives to help citizens recognize and protect themselves

[68] Bele, J. L. (2020). Financial Scams, Frauds, and Threats in the Digital Age. Modern Approaches to Knowledge Management Development, 39.

[69] Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud?. Journal of Economic Behavior & Organization, 198, 250-266.

[70] ibid

[71] Zou, H., Huang, J., Zhang, W., Wu, J., Wu, W., & Huo, L. (2023). The effect of cyberbullying victimization and traditional bullying victimization on suicidal ideation among Chinese female college students: the role of rumination and insomnia. Journal of affective disorders, 340, 862-870.

against cyber threats. Future interventions must prioritize capacity-building for law enforcement and the community to mitigate the risks posed by technology-oriented crimes.

3.3.4. Hacking and unauthorized access

Hacking and unauthorized access to social media accounts have become a significant type of technology-oriented crime in Lideta Sub-City. Victims reported having their accounts breached, leading to the exploitation of personal data and misuse of their online identities. One victim shared,

> *"The hacker started using my profile to send inappropriate messages to my contacts after I lost control of my social media account." (A male victim, age 31.)*

This breach often results in further crimes such as financial fraud, or cyberbullying. Police officers acknowledged the growing frequency of such incidents but pointed out that

> *"We lack the resources and advanced systems needed to track and prevent these crimes"* (Male police officer, 39 years old).

Law enforcement's capacity to respond efficiently is further hampered by obsolete legislation and legal loopholes. In addition to violating privacy, social media account hacking puts individuals at risk for psychological and financial harm. The rights of victims, especially the rights to privacy and personal security, are impacted by unauthorized access to personal data. According to a police officer,

> *"We don't have enough legal tools to fight back against these types of crimes, and the public is not well-informed on how to protect their accounts"* (Male victim, 24 years old).

This aligns with global research showing that inadequate legal frameworks and rapid technological advancements hinder effective law enforcement in cybercrime cases[72]. Furthermore, the emotional impact on victims, such as distress from losing control of their

[72] Smith, L., Chowdhury, M. M., & Latif, S. (2022). Ethical hacking: Skills to fight cybersecurity threats. EPiC Series in Computing, 82(5), 102-111.

online identity, necessitates a stronger emphasis on public awareness and preventive measures.

3.4. Impact of Technology-Oriented Crimes on Human Rights

The most common threat of technology-oriented crimes includes significant violation of fundamental human rights, such as the right to privacy, freedom of expression, and access to justice. Both police officers and victims reported these violations due to technology-related crimes.

3.4.1. Violations of Privacy

Participants consistently reported that technology-related crimes significantly impact individuals' right to privacy. Participant, a police leader, emphasized,

> "*The crime has a significant impact on human rights such as the right to privacy—people usually post private pictures and information on social media without consent*." (Male team leader, police officer, 45 years old)

This breach of privacy through social media is widespread and illustrates how easy it is for individuals' personal information to be exploited. These findings are consistent with the literature, which shows that technology-oriented crimes often lead to violations of fundamental human rights[73]. Privacy breaches, as well as restrictions on freedom of expression, are growing concerns in digital spaces. The results indicate an urgent need for policies that prioritize the protection of human rights in the context of digital crime, as well as stricter enforcement of online harassment laws[74]

3.4.2. Freedom of Expression

Victims of cyberbullying and other technology-related crimes also felt their freedom of expression was infringed upon. One of the respondents noted,

[73] ibid

[74] Weeramantry, C. G. (2023). Justice Without Frontiers: Protecting human rights in the age of technology (Vol. 2). Brill.

"Social media related harassment affected my right to freedom of speech on social media." (25 years old female victim)

This reaction suggests that people are deterred from openly expressing their thoughts online by the fear of being harassed online. These results support research demonstrating that restriction of free speech is frequently the consequence of cybercrimes, especially when people fear harassment or reprisal for voicing their thoughts online. The consequences for freedom of speech and privacy highlight how critical it is to protect these rights online, a worry that is shared by several human rights groups across the world[75]. For law enforcement and policymakers in Lideta Sub-City, the violation of human rights resulting from technology-oriented crimes particularly with regard to privacy and freedom of expression presents a significant problem[76]. This necessitates stricter privacy laws together with legislative changes that offer a defined judicial process for these kinds of offenses. Furthermore, public knowledge[77]

The infringement of human rights due to technology-oriented crimes, particularly concerning privacy and freedom of expression, presents a critical challenge for both law enforcement and policymakers in Lideta Sub-City. This calls for more stringent privacy protections, coupled with legal reforms that provide a clear mechanism for prosecuting these crimes. Additionally, public awareness campaigns should focus on educating citizens about their digital rights and how to protect them. Empowering individuals to take control of their online presence, while simultaneously holding perpetrators accountable, is crucial to protecting human rights in the digital age[78].

3.5. Role of the Police in Protecting Human Rights

The study also looked at how the police are currently defending human rights against crimes involving technology. The majority of police officers surveyed believed that weak legislative frameworks, limited resources, and inadequate training were impeding their efforts.

[75] Reglitz, M. (2020). The human right to free internet access. Journal of Applied Philosophy, 37(2), 314-331.

[76] ibid

[77] ibid

[78] ibid

3.5.1. Limited Knowledge and Training

One of the key challenges faced by the police is the lack of specialized training to handle technology-related crimes. Participant, a team leader, remarked,

> *"I'm not aware of any training programs in Ethiopia connected to technology-related crimes."* (Male police officer, 30 years old)

Other officers had a similar opinion, arguing that police personnel lack the necessary tools to tackle the intricacy of cybercrimes. Numerous studies on cybercrime response have extensively demonstrated law enforcement agents' deficiency in specialized expertise and training[79]. Without the necessary skills and tools, police officers are often unable to keep up with the rapidly evolving nature of technology-related crimes, leaving gaps in both prevention and prosecution[80]. Moreover, the lack of all-encompassing regulations specifically designed to tackle cybercrimes makes it more difficult for the police to adequately uphold human rights, especially in environments with low resources like Lideta Sub-City. The police's inadequate ability to combat technology centered crimes has serious ramifications for the defense of human rights. The necessity for focused training programs that give officers the skills and resources they need to deal with these crimes is urgent in order to improve the efficacy of law enforcement. Policy changes should also concentrate on developing a stronger legal framework that makes technology-related crimes explicitly defined and illegal, giving law enforcement organizations the authority to take decisive action. Enhancing cooperation among law enforcement, IT specialists, and community members may also help the police better protect human rights against cyber-attacks.

3.5.2. Insufficient Legal Frameworks

Another theme that emerged was the inadequacy of the legal system in addressing technology-related crimes. The participant emphasized,

[79] Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1).

[80] ibid

"*I don't believe that the laws and guidelines pertaining to crimes involving technology are sufficient to stop violations of human rights." (Male victim, 28 years old)*

This identifies regulatory gaps that make it more difficult for law enforcement to effectively combat these types of crimes. The results demonstrate that structural problems, such as insufficient legislative frameworks and training, hinder the police's ability to protect human rights in technology-related offenses. These findings are consistent with earlier research that emphasizes the necessity of increased police capability to combat cybercrimes. Comprehensive reform is obviously required, and this must include improved training initiatives and the creation of dedicated cybercrime sections[81]

3.6. Challenges Faced by Police in Combating Technology-Oriented Crimes

Police officers found that fighting technology-related crimes was difficult due to a lack of training, unclear legal frameworks, complicated jurisdictions, and the quick speed at which technology is developing.

3.6.1. Resource Constraints

One of the primary challenges faced by the police is the lack of resources. Participant stated, *we don't have enough sophisticated systems in place to look into crimes involving technology." (Male police officer, 31 years old)*

This emphasizes the requirement for cutting-edge technologies and investigative techniques that will enable law enforcement to more efficiently detect and prosecute cybercrimes. These issues are in line with research findings from other studies that examine the obstacles law enforcement encounters while dealing with cybercrimes. Often mentioned as major problems include jurisdictional difficulties and resource limits, especially in poorer nations where technology infrastructure is still in its infancy[82]. The rapid evolution of technology also means

[81] Shivpuri, D. (2021). Cyber crime: Are the law outdated for this type of crime. International Journal of Research in Engineering, Science and Management, 4(7), 44-49.

[82] ibid

that new forms of crime are constantly emerging, making it difficult for law enforcement agencies to stay ahead.[83]

3.6.2. Rapid Technological Advancements

Another challenge identified was the pace of technological change, which outpaces the police's ability to adapt. As Participant noted,

> *"We are not prepared for these new kinds of crimes since technology is evolving more quickly than we can keep up with it."* (Male police officer, 36 years old)

This implies that as criminals discover new ways to take advantage of developing technologies, the authorities are frequently left behind. These difficulties are typical of a global trend in which law enforcement organizations find it difficult to keep up with the quickly changing landscape of digital crimes[84]. Police officers lack the necessary tools and training to handle the complexity of cybercrime. These results highlight the necessity of providing human and technological resources to improve law enforcement's capacity to tackle crimes involving technology.

As technology becomes more widely available, cybercriminals have greater options, frequently surpassing the ability of law enforcement organizations to successfully combat these threats. Some police officers have acknowledged a weak grasp of technology-related crimes, which exacerbates the problem by reflecting a lack of training and preparation. This result is consistent with earlier research emphasizing the value of specific training for law enforcement in combating cybercrime[85].

The difficulties the police in Lideta Sub-City encounter are a reflection of larger systemic problems with inadequate resources, outdated technology, and weak legislative frameworks. Investing in the creation of dedicated cybercrime units within law enforcement organizations, outfitted with the resources and expertise needed to combat crimes centered around

[83] ibid

[84] ibid

[85] Mayne, R., & Green, H. (2020). Virtual reality for teaching and learning in crime scene investigation. Science & Justice, 60(5), 466-472.

technology, is imperative in order to tackle these issues. In addition, legal changes are required to provide a more thorough framework for combating cybercrime and to guarantee that law enforcement officials have the power and resources to carry out their duties. Cooperation with foreign organizations and technological specialists can also aid in filling in knowledge and resource shortages, empowering law enforcement to more effectively tackle cybercrimes.

3.6.3. Lack of Updated Technological Infrastructure

The absence of modern technological infrastructure is one of the biggest obstacles the police in Lideta Sub-City encounter when trying to combat crimes involving technology. Criminals frequently have access to more sophisticated equipment and methods than law authorities. As one police officer stated,

> *"Because of the age of our systems, we are unable to keep up with the speed at which criminals are adopting new technology and adapting."* (Male team leader, police officer, 38 years old).

It is challenging for police to properly investigate and prevent crimes like hacking, online fraud, and cyberbullying because of this technology gap. The extended exposure of victims to harm is a result of law enforcement's slow response. Criminals benefit from the quick development of technology, while law enforcement falls behind. The lack of state-of-the-art investigative instruments makes it very difficult to find and capture cybercriminals. Global research suggests that in order to close this gap and enable more effective prevention and response to digital crimes, law enforcement organizations need to invest in modern technology[86].

3.7. Strategies to Enhance Police Role in Protecting Human Rights

Police officers and victims proposed a number of initiatives, including specialized training, greater resources, and engagement with stakeholders, in response to the proposed methods to increase the police's capacity to protect human rights in the context of technology-oriented crimes.

[86] ibid

3.7.1. Specialized Training and Resources

Several participants emphasized the need for better training and resources to address technology-related crimes. As suggested by one of the participants,

> *"It's critical to raise knowledge of social media etiquette and online fraud. To investigate these crimes, the police must have sophisticated procedures in place."* (Male victim, 32 years old).

This emphasizes how crucial it is to give law enforcement the resources and expertise they need to properly combat cybercrimes. Allocating resources and providing specialized training are essential elements in strengthening the police's ability to defend human rights against crimes involving technology[87]. Specially, improving the police department with recent technology

3.7.2. Collaboration with Stakeholders

Collaboration with technology experts and other stakeholders was also seen as crucial. Participant recommended,

> *"Working together with interested parties, we must stop these atrocities."* (Male police officer, department leader, 46 years old)

This suggests that the fight against crimes related to technology needs to be multi-sectoral, engaging not only the police but also IT businesses, civil society, and the general public. These current tactics are in line with international best practices for combating cybercrime, which highlight the significance of cooperation between law enforcement, business, and civil society[88]. Collaborative strategies can also help create a more comprehensive and effective approach to digital crime prevention.

Moreover, it has been demonstrated that cooperative strategies including stakeholders like technology corporations, local authorities, and international organizations are successful in

[87] Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 105, 102258.

[88] ibid

improving law enforcement's ability to combat cybercrime[89]. The suggested methods for strengthening police presence emphasize the necessity of a multipronged strategy to counteract cybercrimes. A comprehensive strategy to solve these difficulties must include public awareness campaigns, improved legal frameworks, and sophisticated investigative tools. Furthermore, encouraging cooperation between law enforcement, IT professionals, and community members can aid in bridging the divide between the police's capacity to adequately respond to cybercrime's ever-changing nature and its evolving nature. Law enforcement organizations in Lideta Sub-City can strengthen their ability to defend human rights in the digital era by putting these tactics into practice.

3.8. Summary of Secondary Data Analysis

This research investigates existing data on technology-related offenses in Ethiopia, focusing on the different reported crimes, their frequency, trends, impact on victims, and challenges encountered by law enforcement. Moreover, it evaluates the legal system, pinpointing deficiencies and recommending modifications to enhance the country's capability in addressing cybercrime.

3.8.1. Types of Technology-Oriented Crimes Documented

The analysis of existing data uncovers various prominent technology-related offenses in Ethiopia. Commonly reported online offenses include:

Hacking: defined as gaining unauthorized entry into an individual's or company's networks in order to steal, manipulate, or erase data. It is particularly common in the business and financial industries.

Identity Theft: Cybercriminals often steal personal information such as names and financial information to commit fraud or impersonate others.

Cyber fraud: covers false online stores, scams in mobile banking, and phishing methods.

Cyberbullying and online harassment: it involves individuals being targeted with hurtful comments, threats, and false accusations, particularly on social media platforms.

[89] ibid

Out of these, online fraud and cyberbullying are the most commonly reported issues, particularly in the past five years. Information from police department's shows that cybercrime, specifically financial fraud and crimes linked to social media has been consistently on the rise. For example, instances of fraud in mobile banking have increased by 25% every year, showing the rise in popularity of digital payment platforms in the nation.

Based on the data, incidents of identity theft and hacking were less common five years ago, but have increased in frequency since then. The rise of digital platforms for daily tasks and increased internet usage are responsible for this trend. As digitalization progresses, cybercrimes are becoming increasingly diverse and common, as indicated by the results.

3.8.2. Human Rights Violations

In Ethiopia, crimes centered around technology frequently include grave violations of human rights. Reports of harassment and hacking constitute typical privacy infractions. People frequently experience financial and psychological harm as a result of identity theft or misuse. Ethiopian privacy breaches are generally associated with hacking events that target people's financial and communication data; victims experience emotional suffering in addition to losing access to their online platforms and sensitive information.

Certain crimes involving technology have limited people's ability to express themselves freely, especially when it comes to cyberbullying and harassment. About instance, social media platform victims of cyberbullying say they feel under pressure to self-censor out of concern about more online harassment. Concern over this covert infringement on the right to free speech is developing in Ethiopia, particularly among the younger generation and prominent personalities.

Cybercrime victims frequently suffer serious consequences to their personal security, finances, and emotional well-being[90]. Particularly at stake is financial stability, since victims of internet fraud frequently lose substantial sums of money. According to certain stories, people have lost all of their life savings to con artists using phony mobile banking or online investing options. Others who are victims of identity theft may suffer long-term repercussions including ruined credit and reputational damage.

[90] ibid

3.8.3. Legal Framework and Policy Review on Technology-Oriented Crimes in Ethiopia

The prevalence of technology-related crimes is rising in Ethiopia along with internet use, which presents a big challenge to both individuals and institutions. The Ethiopian government has responded by putting laws in place to minimize cybercrime. Among the laws of note is Cybercrime Proclamation No. 958/2016[91], which was introduced to combat various cyber offenses, including hacking, identity theft, and online fraud[92]. Even if this legal framework is a positive development, an analysis of secondary data indicates that it is still unable to manage the complexity of contemporary cybercrimes.

3.8.3.1. Gaps in the Legal Framework

Although the Cybercrime Proclamation is in place and provides guidelines for technological crime investigation for police and public prosecutor, it has notable deficiencies, especially when it comes to addressing cybercrimes that cross borders. As internet access grows, cybercriminals are operating more across borders, but Ethiopia's laws are not prepared to handle these international risks. Recent sources indicate that Ethiopia lacks any bilateral deals with other nations to aid in global collaboration on cybercrime probes, causing difficulties for Ethiopian authorities in locating cybercriminals operating abroad[93]. Due to the complexity of cross-border cybercrime, more international collaboration is essential, yet the current legal structure does not have this vital component.

Moreover, the current legal structure does not adequately cover emerging cybercrimes such as complex financial fraud and online misinformation campaigns. Despite the increasing frequency of these crimes on a global scale, Ethiopian legislation remains unclear on how to handle prosecution. Online misinformation has been particularly damaging because it can influence public opinion, interfere in politics, and exacerbate ethnic tensions[94]. Not passing

[91] Yilma, K. M. (2021). Cybercrime Lawmaking and Human Rights in Ethiopia. Mizan Law Review, 15(1), 73-106.

[92] Federal Democratic Republic of Ethiopia. (2016). Cybercrime Proclamation No. 958/2016.

[93] ibid

[94] ibid

laws to address these evolving cybercrimes highlights a significant deficiency in the country's legal system, hindering law enforcement's efficacy in responding.

3.8.3.2. Challenges in Enforcement

The enforcement of current laws is a problem, in addition to the shortcomings in combating newly emerging cybercrimes. The examined records demonstrate that even while the Cybercrime Proclamation No. 958/2016 makes a number of cyber acts illegal, there are still unclear rules governing the gathering and storage of digital evidence, which makes enforcement of the law difficult[95]. Although Ethiopian law lacks a comprehensive framework for gathering, storing, or using digital evidence in court, it is essential for prosecuting cybercriminals.

The absence of regulations makes investigations more difficult and makes it more difficult for law enforcement to successfully punish offenders. For example, officers frequently have difficulty protecting the integrity of digital evidence, which is easily altered or deleted in the absence of appropriate procedures. Cases are therefore routinely dropped for lack of proof, depriving victims of justice and allowing offenders to carry on with their operations[96]. The legal framework thus needs to be updated to include detailed guidelines on digital forensics and evidence handling to ensure that crimes are adequately prosecuted.

3.8.3.3. Victim Protections

Ethiopia's legal system has a significant flaw in the lack of proper protections for victims of cybercrime, specifically individuals facing cyberbullying and online abuse. Women and public figures face a high risk of receiving harassment on social media, yet they have limited legal recourse options[97]. Despite including measures to tackle harassment, the Cybercrime Proclamation is often not effectively enforced, and the consequences do not sufficiently reflect the emotional and psychological impact of such offenses.

---

[95] Yilma, K. M. (2016). Comment: some remarks on Ethiopia’s new cybercrime legislation. Mizan Law Review, 10(2), 448-458.

[96] ibid

[97] ibid

The absence of clear laws or rules dealing with cyberbullying and online harassment leaves victims vulnerable to continued mistreatment and inadequate protection from the legal system. Numerous civil society organizations report that a majority of cyberbullying victims opt not to report their experiences because they believe the legal system will not provide sufficient assistance or justice[98]. This emphasizes the urgent necessity for reforms that target the protection of victims and ensuring accountability for offenders.

Victims of crimes focused on technology suffer greatly as a result. For instance, identity theft and hacking victims frequently face financial devastation when their stolen personal information is exploited to perpetrate fraud. Countless people experience bank account lockouts, credit harm[99]. In other instances, individuals who fall prey to cybercrime are deceived into executing substantial financial transactions, only to come to terms with their deception. These crimes have an equally devastating psychological impact; many victims report feeling anxious and helpless.

The effects of cyberbullying and harassment are particularly concerning. Victims, particularly women and marginalized individuals, frequently experience mental distress, lack of social connection, and in severe instances, may resort to self-inflicted harm or taking their own lives. Due to the severe impact, it is crucial for the legal system to offer increased safeguards for victims and implement harsher punishments for perpetrators.[100]. Given the devastating consequences, it is critical for the legal framework to provide stronger protections for victims and impose stricter penalties on offenders.

When it comes to prosecuting crimes involving technology, Ethiopian law enforcement officials encounter a number of difficulties. The inadequate resources and antiquated IT infrastructure are a big problem. Even though some police officers have taken basic cybercrime courses, they lack the resources necessary to thoroughly investigate complex crimes involving digital evidence. Furthermore, the inability of law enforcement organizations

[98] ibid

[99] Nwanne, T. F. I. (2015). Ethiopian Banking System.

[100] ibid

to hire experts with training in digital forensics hinders their capacity to look into and prosecute perpetrators[101].

Jurisdictional issues also impede the effectiveness of law enforcement. Cross-border cybercrimes are frequent; however, Ethiopia lacks the necessary international cooperation agreements to apprehend foreign offenders. Due to this, the nation is now more open to attacks by foreign criminals who can act almost without consequence[102]. Even in cases where they have enough evidence, Ethiopian police frequently fail to prosecute cybercriminals because they lack the capacity to work with foreign law enforcement organizations.

Finally, in order to effectively combat cross-border cybercrimes, Ethiopia needs to make investments in modernizing its law enforcement capabilities and forming global alliances. This entails supplying contemporary technology tools for cybercrime investigation and training police officers in digital forensics. It is also important to develop international cooperation agreements so that Ethiopian law enforcement can work with foreign authorities to track down and apprehend cybercriminals who operate internationally.

CHAPTER FOUR

4. CONCLUSION AND RECOMMENDATIONS

4.1. Conclusion

This research investigated how common, significant, and challenging technology-focused offenses are in Lideta Sub-City, as well as how law enforcement protects human rights from these crimes. The results showed that in Lideta, technology-related crimes such as financial fraud, cyberbullying, hacking, and sharing illegal content are increasing concerns, impacting privacy and freedom of speech. The police in the sub-city encounter multiple challenges, including limited training, insufficient resources, and a weak legal system, which impede their

[101] Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. Commonwealth Law Bulletin, 46(1), 78-109.

[102] ibid

capacity to efficiently prevent and address these crimes. In addition, the research found significant violations of human rights, specifically concerning to privacy and freedom of speech, stemming from these offenses.

The police face additional challenges in dealing with these crimes due to complex jurisdictional issues and rapid technological advancements, making it difficult for them to effectively combat these offenses. Although both police officers and victims acknowledged the severity of these crimes, they noted a shortage of effective enforcement actions by law enforcement, indicating broader systemic problems concerning the prevention of technology-related crimes in Ethiopia.

Despite the Cybercrime Proclamation No. 958/2016 addressing technology-related crimes, there are still notable deficiencies in Ethiopia's legal system. The nation's legal system and legal frame work is not adequately prepared to address cybercrimes that cross borders, misinformation online, and collecting digital evidence. Insufficient protections leave victims of cyberbullying and online harassment vulnerable. To effectively address these offenses, Ethiopia needs to revise its legal system, enhance law enforcement capabilities, and promote collaboration with other countries. The country can only develop a strong response to the increasing threat of cybercrime by tackling these challenges.

Addressing these challenges requires a multifaceted approach involving capacity building, legal reforms, and collaboration with technology experts and community stakeholders. Public awareness initiatives and specialized training for police officers are critical for improving the response to technology-oriented crimes and safeguarding human rights in Lideta Sub-City.

4.2. Recommendations

Based on the study’s findings, the following recommendations are proposed to enhance the capacity of the police in Lideta Sub-City and strengthen the protection of human rights against technology-oriented crimes:

Create tailored training programs for police officers: Research shows that many law enforcement officers do not possess the required expertise to effectively address technology-related crimes. Therefore, it is essential to implement specialized training programs that concentrate on detecting, investigating, and prosecuting cybercrime. Education should address

new cybersecurity risks, issues of privacy, and the safeguarding of human rights in the online domain.

Enhance Legal Systems for Preventing Technology-related crime: The current regulations in Ethiopia concerning technology-based offenses are deemed inadequate for stopping and resolving such crimes. Legal reforms should focus on developing a broader structure and frame work for recognizing, penalizing, and pursuing technology-related crimes**.**

Boost funding for cybercrime teams: The research revealed a shortage of cutting-edge tools and resources for investigating cyber offenses as a significant obstacle. It is crucial allocate sufficient resources for establishing and operating specialized cybercrime units in law enforcement agencies. This involves offering technical tools, forensic software, and personnel dedicated to managing technology-related cases**.**

Promote Collaborative Partnerships: Encourage partnerships: It is essential to cooperate with technology companies, police, and community stakeholders to combat technology-related crimes. Forming alliances with experts in technology, cybersecurity professionals, and human rights organizations can bridge knowledge and resource disparities. These partnerships should include joint awareness efforts and capacity-building programs to educate the public about online safety and prevent cybercrime.

Enhance Public Awareness Campaigns: To protect individuals from becoming victims and to encourage responsible conduct online, it's critical to raise awareness of technological-oriented crimes. Public education campaign should focus on people's right in digital spheres and the risk of cyberbulling, online fraud, and other technological crimes. To ensure that these initiatives reach a broad audience, it is imperative to involve local groups, schools, and community leaders.

Regular Policy Reviews and Updates: Law enforcement organizations and legislators must regularly review and update regulations pertaining to technology focused crimes due to the rapid advancements in technology and cyber threats. Legal and law enforcement operations will remain effective and up to date if existing methode are routinely evaluated and new regulations are implemented in response to technological advancements.

BIBLIOGRAPHY

Abaje, O. (2024). Cybercrime Threats and Trends in Ethiopia: Critical Legal Analysis. Wallaga University Journal of Law, 1(2), 18-33.

Abiyou Girma(2015,June 15) The Police and Human Rights in Ethiopia. Human Rights,Public Policy and Law Blog.https://www.abyssinialaw.com/blog/the-police-and-human rights-inEthiopia.

Aineah, A. (2022). News processes, opportunities and challenges in converged Kenyan newsrooms: a case study of Standard Group Plc.

Alemayehu, D. (2022). Cybersecurity and legal frameworks in Ethiopia: Challenges and future directions. *Journal of Law and Technology*, 10(2), 56-78.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1).

Ayalew, Y. E. (2020). Assessing the limitations to freedom of expression on the internet in Ethiopia against the African Charter on Human and Peoples' Rights. African Human Rights Law Journal, 20(1), 315-345.

Bele, J. L. (2020). Financial Scams, Frauds, and Threats in the Digital Age. Modern Approaches to Knowledge Management Development, 39.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Brüggemann, S., Kutlu, N., Müller-Török, R., Prosser, A., Ručinská, S., Szádeczky, T., & Vrabie, C. (2022). A scientific basis for a policy fighting fake news and hate speech. OCG/Facultas, 101.

Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud?. Journal of Economic Behavior & Organization, 198, 250-266.

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 105, 102258.

Computer Hope (2023, January 10) Computer Crime. http://www.computerhope.com/jargon/c/compcrim.htm.

Creswell, J. W., & Poth, C. N. (2017). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.

Demetis, D. (2023). Organised crime-the cyber dimension. A Research Agenda for Organised Crime, 177-194.

Dron, J. (2022). Educational technology: what it is and how it works. AI & SOCIETY, 37(1), 155-166.

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. Commonwealth Law Bulletin, 46(1), 78-109.

Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. Journal of Big Data, 11(1), 118.

FDRE Constitution (1995). Constitution of Federal Democratic Republic of Ethiopia.

Federal Democratic Republic of Ethiopia. (2016). Cybercrime Proclamation No. 958/2016.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. British Dental Journal, 204(6), 291-295.

Harvey,L.(2012-2020). Researching the real world https://www.qualityresearchinternational.com /methodology /RRW1pt1Introduction.php

Haugen,Hans Morten(2012,February 1),Technology and Human Rights Friends or Foes?, Highfighting Innovations Applying to Natural Resources and Medicine, Human Rights Series No.1,William Schabas,ed.,Republic of Letters Publishing, https://ssrn.com/abstract=1991058.

Jimma, E. (2022). College of Law and Governance School of Law LLM in Human Rights and Criminal Law (Doctoral dissertation, Jimma University).

Kovacich, G. L., & Boni, W. C. (2011). High-technology crime investigator's handbook: Establishing and managing a high-technology crime prevention program. Elsevier.

Larrañaga, M. G., Iglesias, E. J., & Aizpuru, N. L. (2023). Bullying and cyberbullying: Victimisation, harassment, and harm. The need to intervene in the educational centre. Revista Española de Pedagogía, 77(273), 14.

Mayne, R., & Green, H. (2020). Virtual reality for teaching and learning in crime scene investigation. Science & Justice, 60(5), 466-472.

McGuire, M. R. (2022). Crime, Control and the Ambiguous Gifts of Digital Technology. The SAGE Handbook of Digital Society, 35.

Mehari, S. A. Implications of the Ethiopian Computer Crime Proclamation on the Enjoyment of Human Rights.

Nebiat, L. (2017). The Legal and Institutional Framework for the Corporate Governance of State-Owned Enterprises in Ethiopia (Doctoral dissertation).

Nielsen, J., & Keasling, J. D. (2016). Engineering cellular metabolism. Cell, 164(6), 1185-1197.

Niezen, R. (2020). Human Rights: The Technologies and Politics of Justice Claims in Practice. Stanford University Press.

Nosál, J. (2023). Crime in the Digital Age: A New Frontier. In The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network (pp. 177-193). Cham: Springer International Publishing.

Omidosu, J. (2023). A social-technical harm-based taxonomy of online hate in South Africa.

Otele, O. (2021). Kenya's data protection regime: challenges and future prospects. journal of African politics, 1(1), 66-88.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed-method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), 533-544.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic sciences, 2(2), 379-398.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic sciences, 2(2), 379-398.

Prahassacitta, V., & Harkrisnowo, H. (2021). Criminal disinformation in relation to the freedom of expression in Indonesia: A critical study. Comparative Law Review, 27, 135-165.

Reglitz, M. (2020). The human right to free internet access. Journal of Applied Philosophy, 37(2), 314-331.

Rutenberg, I., & Sugow, A. (2020). Regulation of the Social Media in Electoral Democracies: A Case of Kenya. SOAS LJ, 7, 301.

Saleem, S., Khan, N. F., Zafar, S., & Raza, N. (2022). Systematic literature reviews in cyberbullying/cyber harassment: A tertiary study. Technology in Society, 70, 102055.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. Education for Information, 22(2), 63-75.

Shivpuri, D. (2021). Cyber crime: Are the law outdated for this type of crime. International Journal of Research in Engineering, Science and Management, 4(7), 44-49.

Smith, L., Chowdhury, M. M., & Latif, S. (2022). Ethical hacking: Skills to fight cybersecurity threats. EPiC Series in Computing, 82(5), 102-111.

Smith, L., Chowdhury, M. M., & Latif, S. (2022). Ethical hacking: Skills to fight cybersecurity threats. EPiC Series in Computing, 82(5), 102-111.

Smith, R. K. (2022). International human rights law. Oxford University Press.

Syed Muhammed(2016,July) Methods of Data Collection. https://www.researchgate.net/publication/325846997_methods_of_data_collection

Symeou L. and Lamprianou I. (2008). Research Approach and Methodology, p 2-10. http://www.relabs.org/rsearch.

Tadesse, H. (2023). Law enforcement challenges in combating cybercrime in Ethiopia. Ethiopian Journal of Criminal Justice, 15(3), 115-133.

Thomas, K. V. (2021). The Role of Science & Technology in Law–Enforcement. The Indian Police Journal, 35.

Trierweiler, M. K. (2021). Development of an IT-supported anti-fraud-framework for SMEs: An architectural concept for risk management using the'Man-Technology-Organization 'approach. In STPIS (pp. 204-215).

U.S. Department of state (2023, March 20), 2022 Country Reports on Human Rights Practices:Ethiopia. https://www.state.gov/reports/2027 country-reorts-on-human-rights-practices/

Unite Nations General Assembly Resolution 34/169 (1997, December 17) Code of Conduct for Law Enforcement Officials.

United Nations (1948). Universal Declaration of Human Rights.

Wario Elemo(2020,June).Police Reform and Human Rights Protection in Ethiopia:The case of Federal PoliceCrimeInvestigationBureau.p7 .http://etd.aau.edu.et/bitstream/handle/123456789/22277/Wario%20Elemo%20Final%20Thesis%20paper.pdf?sequence=1&isAllowed=y

Weeramantry, C. G. (2023). Justice Without Frontiers: Protecting human rights in the age of technology (Vol. 2). Brill.

Yeshimar a.b, Asnake, Tadesse(2023, January 28). Analyzing Physical and Socio-economic factors for property crime incident in Addis Ababa, Ethiopia. Published online https://doi/10/0/6/j.heliyon2023

Yilma, A. (2020). The psychological impact of cyberbullying on victims in Ethiopia. Ethiopian Mental Health Journal, 8(1), 22-37.

Yilma, K. M. (2021). Cybercrime Lawmaking and Human Rights in Ethiopia. Mizan Law Review, 15(1), 73-106.

Yohannes, M. (2021). Digital evidence collection and the legal framework in Ethiopia: Current gaps and future prospects. Cyber Law Review, 5(4), 102-118.

Zeynu, H. J. (2022). Human Rights Focused Regional Police Reform Guidance in Ethiopia. Hawassa UJL, 6, 130.

ANNEX

DATA COLLECTION TOOL

Interview Guide for Police Officers and Victims

Introduction:

Thank you for agreeing to participate in this study. The purpose of this interview is to explore your experiences and perspectives related to technology-oriented crimes, such as hacking, cyberbullying, online fraud, and the dissemination of false information. Your responses will help us understand the role of the police in protecting human rights in Lideta Sub-City. The interview will take approximately 45–60 minutes. All information will be kept confidential, and your identity will not be disclosed.

Section 1: Background Information

1. Could you please state your age, gender, and current position?

2. For police officers: How many years have you worked in law enforcement?

3. For victims: Could you describe the type of technology-oriented crime you experienced? How did it affect you?

Section 2: Prevalent Technology-Oriented Crimes

1. From your experience, what are the most common technology-related crimes in Lideta Sub-City? (For police officers and victims)

2. In your opinion, how frequently do these crimes occur? Can you give any specific examples?

3. For police officers: How do you and your colleagues identify and respond to these crimes?

Section 3: Impact on Human Rights

1. How do technology-oriented crimes, such as hacking or online fraud, affect individuals' human rights (e.g., privacy, freedom of expression)?

2. For victims: How has your experience impacted your rights or sense of security? Did it affect your privacy, freedom of speech, or other rights?

3. For police officers: Do you think law enforcement in Lideta Sub-City has been effective in protecting these rights? Why or why not?

Section 4: Role of Police in Combating Technology-Oriented Crimes

1. What steps do the police take when investigating technology-oriented crimes? Could you describe any specific processes or strategies?

2. How do you think the current legal framework in Ethiopia addresses these crimes? Do you find the laws sufficient?

3. For police officers: Are there any specialized training programs for handling cybercrime cases? If so, have you participated in any?

Section 5: Challenges in Combating Technology-Oriented Crimes

1. What challenges do you face in preventing or solving technology-oriented crimes (e.g., lack of resources, training, legal support)?

2. For victims: How easy or difficult was it to report your case to the police? Were the authorities helpful?

3. For police officers: What is the most significant obstacle in dealing with these crimes effectively?

Section 6: Recommendations and Solutions

1. In your opinion, what improvements or strategies could be implemented to better protect human rights against technology-related crimes?

2. What role could community members or other stakeholders (e.g., technology experts, policymakers) play in preventing these crimes?

3. What recommendations do you have for improving the police's response to technology-oriented crimes?

Secondary Data Review Tool (For Reviewing Reports and Documents)

Key Data Points to Collect:

- Types of Technology-Oriented Crimes Documented:
- What specific types of cybercrimes are reported (e.g., hacking, identity theft, online fraud, cyberbullying)?
- How frequently do these crimes appear in the reports?
- Are there any trends in the types or frequency of crimes over time?
- Does the document/report mention any direct or indirect violations of human rights, such as privacy breaches or restrictions on freedom of expression?
- How are the victims affected in terms of security, personal information, or financial stability?
- Are there any documented challenges faced by the police in preventing or solving technology-related crimes?
- Legal Framework and Policy Review:
- Are there any mentions of Ethiopia's legal policies on technology-oriented crimes?
- What are the most common challenges reported in terms of law enforcement's ability to deal with technology-oriented crimes (e.g., lack of resources, outdated infrastructure, and jurisdictional issues)?