
**Addis Ababa University**

**School of Law**

# The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia

By:

**Samuel Worku**

Advisor:

**Mesfin Beyene** (Assistant Professor)

Addis Ababa, Ethiopia

May 2024.

**Addis Ababa University**

**School of Law**

# The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia

By:

**Samuel Worku**

ID No: GSR/9277/14

Advisor:

**Mesfin Beyene** (Assistant Professor)

This thesis is submitted in partial fulfillment of the requirements for the Master of Law Degree (LL.M) in Human Rights Law at Addis Ababa University.

Addis Ababa University

School of Law

May 2024

**Approval Sheet by the Board of Examiners**

The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia

I hereby declare that this thesis is my original work and all source materials used in this work have been properly recognized.

**Declared by: Samuel Worku**

**Approved By:**
**Advisor: Mesfin Beyene** (Assistant Professor)

**Examiners**

**1.**_____ _____

**2.**_____ _____

## Contents

**Acknowledgment**

I am grateful to everyone who supported me throughout the writing of this thesis. My deepest thanks to my advisor, Ass. Prof. Mesfin Beyene, whose expertise and insightful guidance were invaluable throughout this research.

**Acronyms**

| | |
|---|---|
| ACHPR | African Charter on Human and People's Right |
| CBE | Commercial Bank of Ethiopia |
| ECA | Ethiopia Communication Authority |
| DPAs | Data Protection Authorities |
| ECJ | European Court of Justice |
| EPRDF | Ethiopian People's Revolutionary Democratic Front |
| FISA | Foreign Immunity and Sovereignty Act |
| EUGDPR | European Union General Data Protection Regulation |
| ICCPR | International Covenant on Civil and People's Rights |
| INSA | Information Network Security Agency |
| NIS | National intelligence Service |
| PDPP | Personal Data Protection Proclamation No. 1321/2024 |
| UDHR | Universal Declaration on Human Rights |

**Abstract**

This thesis examines the evolving legal landscape governing personal data protection in the age of growing surveillance in Ethiopia. It identifies that due to the lack of sufficient procedural privacy safeguards, abuse of laws to achieve political purposes, and the existence of poor oversight mechanisms that fail to regulate the extensive surveillance powers granted to police and security service agencies, human rights including, the privacy rights of citizens are impacted. However, the personal data protection farmwork introduced by the new Personal Data Protection Proclamation addresses some of these gaps.

Despite the new law, however, significant gaps including lack of independent regulatory farmwork remain. The study offers recommendations to enhance the personal data protection framework including, advocating for rigorous implementation of the Personal Data Protection Proclamation, establishment of independent oversight mechanisms, and establishment of regular reporting mechanism on surveillance activities to ensure the use of surveillance powers in transparent, accountable, and proportionate manner.

## Chapter One

### 1.1. Background of the Study

In the modern era, the concept of the right to privacy has evolved significantly, particularly in the face of rapidly advancing technological capabilities in surveillance and data collection. The right to privacy is a fundamental human right, recognized in various international human rights instruments, such as the Universal Declaration of Human Rights[1] and the International Covenant on Civil and Political Rights[2] etc. Ethiopia adheres to key global and regional human rights agreements, such as the International Covenant on Civil and Political Rights (ICCPR). These international accords define essential freedoms, encompassing privacy, personal security, freedom of movement, protection against random arrest and detention, and liberties related to opinion, expression, and assembly.

ICCPR's Article 17 mandates that individuals should not face random or illegal intrusions into their privacy, family, home, or communications, affirming everyone's entitlement to legal defense against such violations.[3] Historically, privacy was primarily concerned with physical intrusion.[4] However, the advent of digital technology has drastically expanded its scope to include data protection and informational privacy. Additionally, the term "correspondence" has been expanded by the special rapporteur on freedom of expression to include all communication forms, whether digital or physical.[5] The Human Rights Council, the UN's premier human rights institution, declared in 2011 that rights available offline must be equally upheld online.[6] Although these rights are subject to limits, any restriction must adhere to international legal standards, being lawful, necessary for a legitimate purpose, and specifically and narrowly applied to serve that purpose.[7]

---

[1] Universal Declaration of Human Rights, art 12 (UDHR).

[2] International Covenant on Civil and Political Rights, art 17 (ICCPR).

[3] ICCPR, art 17.

[4] Debbie V S Kasper, 'The Evolution (Or Devolution) of Privacy' (2005) 20(1) Sociological Forum 69, 71.

[5] UN General Assembly, 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development', Human Rights Council Seventeenth session, Agenda item 3, A/HRC/17/27 (2011) 16.

[6] Ibid 7.

[7] Ibid 8. These principles are called principles of predictability, transparency, legitimacy, necessity, and proportionality.

Accordingly, surveillance of communications is intrinsically invasive and should only be executed under exceptional circumstances, with judicial oversight.[8] Laws must clearly define the surveillance's extent, duration, and conditions, the qualifications for ordering it, the entities authorized to execute and oversee it, and the legal recourse available. Clarity and precision in legal provisions are essential to ensure individuals can anticipate their application.[9] The proportionality principle demands that surveillance should not be used if less invasive options exist and must be balanced against the interest it aims to protect. Even in counterterrorism efforts, as stated by the special rapporteur on human rights and counterterrorism, surveillance must avoid secrecy, undergo effective oversight, and receive authorization from an independent entity.[10]

These principles and guidelines serve as a framework for countries to align their domestic policies with international human rights standards, ensuring that measures taken in the name of security or public order do not unjustifiably infringe upon individual rights. Human rights instruments advocate for a balanced approach where the protection of national security and public order does not overshadow the fundamental rights and freedoms of individuals. Accordingly, a legal environment where privacy, freedom of expression, and the right to information are respected and protected, ensuring that any limitations on these rights are justified, necessary, and proportionate is necessary to protect human rights including right to privacy. Adherence to these principles not only fosters trust in governmental institutions but also promotes a more open and democratic society where individuals can freely express themselves and engage in meaningful discourse without fear of reprisal or censorship.

Despite Ethiopia's adherence to international human rights standards and recognition of the right to privacy within its constitution, the country has historically lacked comprehensive laws specifically designed for the protection of personal data, relying instead on dispersed and sector-specific legislation. This deficiency has made the practical application of privacy rights, particularly in the digital realm, a complex challenge.[11]

---

[8] Ibid 21.

[9] Ibid 16.

[10] Ibid 10.

[11] Eyerus Fiseha & Sintayehu Abebe, 'Ethiopia is Moving Towards Data Protection', (*Renew Capital*, 8 Jan 2022) <www.renewcapital.com/newsroom/ethiopia-is-moving-towards-data-protection> accessed 13 October 2023.

The recent enactment of a comprehensive personal data protection law marks a significant development, aiming to address these challenges by establishing clearer guidelines and stronger enforcement mechanisms. This new legal framework is crucial as Ethiopia continues to advance digitally, underscored by initiatives like the Digital Ethiopia 2025 strategy, which raises pressing questions about the balance between state surveillance for security purposes and the protection of individual privacy rights.[12]

Ethiopia's surveillance landscape has been shaped by various factors, including its security challenges, governance style, and technological advancements.[13] The government has historically employed surveillance as a tool allegedly for maintaining public order and national security as well as to attack opposition political parties.[14] The use of surveillance technologies in Ethiopia, such as internet monitoring, phone tapping, and the use of surveillance cameras in public spaces, has been a subject of considerable debate.[15] While these tools can play a crucial role in combating crime and terrorism, they also pose risks to citizens' privacy and other human rights, especially when lacking adequate oversight frameworks.

The paper examines the evolving legal landscape governing personal data protection in the age of growing surveillance in Ethiopia, identifies key challenges, and offers insights on how to address these issues. By conducting a thorough analysis of surveillance laws and the new Personal Data Protection Proclamation, the paper provides recommendations that could help enhance the country’s personal data protection and privacy laws.

---

[12] Ibid.

[13] Saskia Brechenmacher, ‘Civil Society Under Assault: Repression and Responses in Russia, Egypt, and Ethiopia' (2017) Carnegie Endowment for International Peace.

[14] Human Rights Watch, 'They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia' (March 2014) <www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia> accessed 5 October 2023.

[15] Ibid.

### 1.2. Problem Statement

In a world where data is often described as the new oil[16], the implications of data collection, processing, and surveillance have become global concerns. Ethiopia, like many developing nations, is at a crossroads of technological advancement and socio-political evolution. In recent years, the nation has witnessed a rapid increase in digital connectivity and technological adoption, which has brought forth significant benefits in terms of economic and social development.[17] However, this digital transformation has also ushered in a new era of surveillance capabilities, both in the hands of the state and private entities.[18] This evolution raises critical questions about the right to privacy, an issue that has not been comprehensively addressed in the Ethiopian context.

Although Ethiopia's constitution recognizes the right to privacy, the practical application of this right, particularly against the backdrop of increasing digital surveillance, is fraught with complexities.[19] In Ethiopia, understanding privacy is crucial not only as a defense against unwarranted state intrusion but also as a safeguard against potential exploitation by private entities.

Despite the existence of some literatures authored on data privacy, personal data protection focusing on the dispersed laws and data subject rights, there is a noticeable lack of research exploring the interplay and impact of surveillance on personal data protection. This gap extends to a detailed analysis of the new personal data protection law, which is poised to reshape the legal landscape for personal data protection in Ethiopia.[20] Notable works by Kinfe offer invaluable insights into theoretical aspects of data protection and critique the gaps in data protection and data privacy laws, especially in areas like the compatibility of Ethiopian data protection laws with global best practices, their specific provisions, and suggestions for amendments. This paper aims

---

[16] Christoph Stach, 'Data Is the New Oil–Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration' (2023) 15 Future Internet 1 < www.mdpi.com/1999-5903/15/2/71> accessed 03 October 2023.

[17] UNCTAD, 'Ethiopia's drive to advance digital transformation' UNCTAD/BRI PROJECT/PB 02 (April 2022) 2 <https://unctad.org/system/files/information-document/BRI-Project_policy-brief-02_en.pdf> accessed 03 October 2023.

[18] Saskia Brechenmacher (n 14) 70.

[19] Ibid.

[20] Most research on the Ethiopia data protection and data privacy legal frameworks are conducted by Dr. Kinfe Michael Yilma.

to address these critical issues, contributing to the discourse on privacy and data protection in Ethiopia.

### 1.3. Research Questions

I. To what extent do Ethiopia's current data protection laws safeguard personal data amidst increasing surveillance?

II. What legal gaps and inconsistencies exist in Ethiopia's surveillance and personal data protection frameworks that might undermine the protection of personal data?

III. How can Ethiopia strengthen its legal frameworks to enhance the protection of personal data?

### 1.4. Objectives

- Investigate the adequacy of existing Ethiopian laws in ensuring personal data protection, especially in the context of increased surveillance and data collection.
- Identify specific legal gaps and discrepancies that expose vulnerabilities to surveillance in the current framework.
- Offer evidence-based recommendations to strengthen Ethiopia's legal frameworks for enhanced protection of personal data amidst increasing surveillance practices.

### 1.5. Scope of the Study

This study conducts a thorough examination of data protection rights in Ethiopia's digital landscape, focusing on the country's legal framework governing surveillance. The research primarily relies on doctrinal legal analysis and literature review scrutinizing the existing legal provisions for privacy and data protection, evaluating their sufficiency for human rights protection. However, this paper does not engage in an extensive exploration of the theoretical and philosophical underpinnings of human rights, particularly the right to privacy in its traditional understanding. Instead, it will focus on issues specifically related to surveillance, personal data protection, and privacy.

### 1.6. Significance of the Study

This thesis has significance to policy and legal development as it contributes to policy and legal development by identifying gaps and strengths within these frameworks, and offering substantive recommendations to inform policy, guide stakeholder actions, and enhance public understanding

and participation in the discourse on privacy and data protection. Additionally, it brings to the forefront the implications of surveillance and data collection practices on individual freedoms and rights. By doing so, it supports advocacy efforts aimed at safeguarding privacy rights in Ethiopia and beyond.

## 1.7. Research Methodology

### 1.7.1. Research Design

This study adopted a qualitative doctrinal research design to perform a comprehensive examination of Ethiopia's data protection and privacy laws in alignment with international standards. The doctrinal nature of this research means that it focuses on an in-depth analysis of the legal framework governing surveillance and data protection laws in Ethiopia and pertinent secondary sources of literature suitable for the study.

### 1.7.2. Data Collection Methods

The data collection prioritized a literature review, drawing from sources such as academic journals, legal documents, governmental reports, and publications by human rights organizations. The focus was on Ethiopian surveillance and privacy laws, and international human rights laws. This includes an in-depth legal document analysis concerning privacy, surveillance, data protection, and human rights, as well as a review of relevant international legal frameworks Ethiopia is engaged with. Accordingly, the Ethiopian constitution, relevant proclamations, and regulations as well as international and regional human rights instruments have been employed in the research.

### 1.7.3. Data Analysis

The analysis utilized legal analysis techniques to interpret Ethiopian laws and policies in the realms of surveillance, data privacy, and personal data protection, evaluating their adequacy in terms of protecting personal data in the increasing surveillance practice.

### 1.7.4. Ethical Considerations

The researcher-maintained objectivity throughout the study, avoiding biases towards any group or opinion, to uphold the impartiality and ethical rigor of the research.

### 1.8. Limitation of the Study

The researcher faced challenges while conducting the research including accessing information, and lack of detailed literatures on the area specially regarding the Ethiopian context. The researcher faced challenges in accessing detailed and sensitive information regarding government surveillance practices, policies, and their implementation due to national security concerns and bureaucratic hurdles. Therefore, some analyses may rely on available public data and secondary sources, which may not capture the full picture.

Additionally, the research process was impacted by the legislative evolution of the new Personal Data Protection Proclamation. The law underwent several amendments before being ratified in April 2024, each alteration forcing the researcher to revise the paper to accurately reflect the latest legal framework.

### 1.9. Primary Literature Review

Despite the existence of some literatures authored on data privacy, personal data protection focusing on the dispersed laws and data subject rights, there is a noticeable lack of research exploring the interplay and impact of surveillance on personal data protection. However, Kinfe Micheal Yilma, in his article "Data Privacy Law and Practice in Ethiopia," makes the case that social, economic, and political reasons contribute to Ethiopians' lack of interest in privacy.[21] He argued that the prevalent communal lifestyle in Ethiopia, economic constraints, and the absence of a strong human rights culture and the legacy of authoritarian regimes has contributed to a societal norm where privacy is not highly valued. Kinfe identifies unregulated data collection practices, unregulated surveillance practices, and privacy-unfriendly laws as major threats to privacy in Ethiopia.

Additionally, another research titled "Privacy and Personal Data Protection in Ethiopia," by the same author evaluated how well Ethiopia's current legislative and regulatory frameworks uphold privacy and data protection.[22] Kinfe analyzed national laws and policies pertaining to the protection of personal data and privacy and makes the case that privacy is not fully conceptualized in Ethiopia, with current laws restricting private rights even in the face of constitutional guarantees.

---

[21] Kinfe Micheal Yilma, 'Data Privacy Law and Practice in Ethiopia' (2015) *International Data Privacy Law*, Advance Access published 24 May 2015.

[22] Yilma Kinfe Michael, 'Privacy and Personal Data Protection in Ethiopia' (Promoting Effective and Inclusive ICT Policy in Africa, September 2018)

The study offers examination of Ethiopia's privacy and data protection laws, highlighting critical gaps and challenges It underscores the urgency of adopting comprehensive legal frameworks and establishing dedicated oversight institutions. Overall, this research is an invaluable tool for comprehending the nuances of data protection and privacy in Ethiopia and offers a solid foundation for further research and policy development.

Alebachew B. Enyew, in his research titled "Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia," examines the legal protection accorded to privacy by domestic laws.[23] The paper provides a thorough examination of Ethiopia's legal landscape concerning privacy and data protection and identified the absence of specific privacy legislation as a key challenge to protection of personal data in Ethiopia. Alebachew highlights the urgent need for Ethiopia to adopt comprehensive privacy laws aligned with international best practices to enhance the protection of personal data and support the country's socio-economic transformation. However, it should be noted that this paper was written in 2009, and the Ethiopian legal framework for personal data protection has since evolved, with new legislations promulgated that directly and indirectly governs issues related to personal data protection.

Dadimos Haile, in the DataGuidance overview on Ethiopia's data protection, highlights that Ethiopia lacks a comprehensive data protection law.[24] The article lists and indicates the provisions of the scattered laws and sector-specific regulations that regulate data protection directly and indirectly. However, the article does not provide a thorough analysis of the legislation and their implications on data protection.

In "Comments: Some Remarks on Ethiopia's New Cybercrime Legislation," Kinfe Micheal Yilma provides a commentary on the cybercrime legislation, highlighting some of the challenges that lie ahead in the course of implementing the law.[25] He points out the potential threats the Cybercrime legislation poses to the right to privacy. Among other issues, Kinfe highlights that the powers of sudden searches and virtual forensic investigation accorded to the Information Network Security Agency have a chilling effect on privacy rights, further complicated by the lack of judicial

[23] Alebachew B Enyew, 'Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia' (LLM thesis, University of Oslo 2009)

[24] Dadimos Haile, 'Ethiopia - Data Protection Overview' (DataGuidance) https://www.dataguidance.com/notes/ethiopia-data-protection-overview accessed 30 June 2024.

[25] Kinfe Yilma, 'Comments: Some Remarks on Ethiopia's New Cybercrime Legislation' (2016) 10(2) *Mizan Law Review* 453.

oversight. He also argues that the duty to report imposed on service providers has the potential to prompt preemptive monitoring of communications on their networks under the threat of penalties for non-cooperation.

Despite the existing literature on the general framework of data privacy, there has been no systematic analysis of the connection between personal data protection and surveillance in a comprehensive manner. Furthermore, these works have not addressed recent legislation, particularly the new Personal Data Protection Proclamation and the regulation of personal data under the updated legal framework. This research aims to fill this gap by analyzing laws pertinent to personal data protection, including the new Personal Data Protection Proclamation, and examining their shortcomings. Additionally, it will highlight surveillance practices and their impacts on human rights, providing recommendations to improve the legal framework for personal data protection.

## Chapter two

# 2. The Intersection of Data Protection, Privacy, Human Rights, and Surveillance Theories

## 2.1. Overview of the Nature and Justification of Privacy

The right to privacy is a complex and multifaceted concept that has been explored extensively by major philosophers and theorists throughout history. Privacy is recognized and upheld based on a variety of factors, including economic and political contexts, property rights, and other essential human rights such as autonomy and dignity.[26] Scholars' perspectives on privacy vary: some describe it negatively, focusing on the right to solitude/left to be alone,[27] while others perceive it positively, highlighting the right to control personal information,[28] transfer these rights, and enjoy emotional freedom,[29] including the rights to love and form relationships.

Historically, privacy has been acknowledged as a right necessitating state protection. This involves distinguishing between private and public spheres and encompasses rights like the enjoyment of one's property without external intrusion and the right to be alone.[30]

In the ancient time such as ancient Greece, Aristotle touched on aspects of privacy in his discussions of the public and private spheres.[31] He distinguished between the polis (public life) and oikos (private life), emphasizing that a balance between these realms is crucial for a well-functioning society.[32] Moreover, privacy in the Roman Law was more about property rights and less about individual autonomy. The concept of "domus" (home) as a private sanctuary was recognized, where certain legal protections were afforded.[33] Additionally, enlightenment thinkers

---

[26] Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008) 12.

[27] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193, 195.

[28] Ibid 219; see also Dorothy J. Glancy, 'The Invention of the Right to Privacy' (1979) 21 Arizona Law Review 23.

[29] H. J. McCloskey, 'Privacy and the Right to Privacy' (1980) 55 Philosophy 17, 20.

[30] Louise Marie Roth, 'The Right to Privacy Is Political: Power, the Boundary between Public and Private, and Sexual Harassment' (1999) 24(1) Law & Social Inquiry 50.

[31] Olga Mironenko Enerstvedt, 'Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles' (2017) 37 Law, Governance and Technology Series (Springer) 23.

[32] Ibid.

[33] Kate Cooper, 'Closely Watched Households: Visibility, Exposure, and Private Power in the Roman "Domus"' (2007) Oxford University Press 5.

such as John Locke, in his treatise on government, implied a right to privacy as part of the broader rights to life, liberty, and property.[34] His philosophy laid the groundwork for viewing privacy as integral to individual freedom. Kantian ethics, focusing on autonomy and respect for persons, indirectly supports the right to privacy emphasizing on the intrinsic worth of the individual can be tantamount to respect for personal privacy.[35] However, utilitarianists such as Jeremy Bentham and John Stuart Mill's expression of privacy in the context of the greatest happiness principle could justify invasions of privacy if they result in the greater good for the majority. According to Mill

> The sole end for which mankind are warranted, individually or collectively in interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant.[36]

Some scholars such as Warren and Brandies, also describe privacy from the perspective of seclusion from interference. They consider privacy as a legal right essential for personal dignity and autonomy by prohibiting external actors to the person whose privacy is at stake to be left alone (the right to be let alone).[37] Protection of the private realm of a person in contradistinction of the public sphere may be important for personal development away from the public eye.[38] Privacy also involves legal and political perspectives and some scholars such as Alan Westin, defined it as the ability of individuals to control information about themselves, framing it as a function of modern democratic societies.[39] It requires modern states to support individual autonomy and personal development, essential in the digital age to protect against surveillance and data control.[40]

---

[34] John Locke, 'Two Treatises of Government' (1860) McMaster University Archive of the History of Economic Thought 197.

[35] Warren and Brandeis (n 27) 196.

[36] Raymond Wacks, *Privacy: a very short introduction* (2nd edition, Oxford University Press 2010) 34.

[37] Warren and Brandeis (n 27) 865; Kenneth Einar Himma, 'Privacy Versus Security: Why Privacy is Not an Absolute Value or Right' (2007) 44(1) San Diego Law Review 865.

[38] Raymond Wacks (n 36) 36; Alan F. Weinstein, 'Privacy and Freedom' (1968) Washington and Lee Law Review 25.

[39] Alan F. Westin, 'Privacy and Freedom' (1968) 25(1) Washington and Lee Law Review 170.

[40] Julie E. Cohen, 'What is Privacy For?' (May 2013) 126(7) Harvard Law Review 1910.

Bygrave identifies four primary approaches to defining privacy: the concept of non-interference, the idea of limited accessibility, the principle of information control, and a composite approach that integrates elements of the first three while associating privacy strictly with personal, intimate, or sensitive aspects of individuals' lives.[41] These foundational perspectives are broad, encompassing numerous variations and interpretations. Moor and Tavani further refine these ideas, introducing theories of non-intrusion, seclusion, limitation, and control, and proposing an integrative framework known as the Restricted Access/Limited Control (RALC) theory.[42] This comprehensive theory encompasses three core elements: a conceptual understanding of privacy, a rationale for its protection, and strategies for its management.[43] Additionally, Solove expands the discourse by introducing the notions of privacy-as-secrecy and privacy-as-intimacy, which align with the four fundamental categories.[44] Solove's taxonomy categorizes privacy issues into four groups: information collection, processing, dissemination, and invasion.[45]

According to Judith Jarvis Thomson, privacy is a derivative of property rights and bodily autonomy, suggesting that privacy rights emanate from more fundamental rights.[46] Charles Fried, conceptualizes privacy as critical for emotional release, moral autonomy, and the development of relationships.[47] He argues that privacy is essential for love and trust.

However, theorists who describe privacy through the economic lens of cost-benefit analysis such as Richard Posner argue that privacy can shield wrongdoing and reduce transparency.[48] Feminist

---

[41] Lee A Bygrave, 'The Place of Privacy in Data Protection Law' (2000) 24(1) UNSW Law Journal 279.

[42] Olga Mironenko Enerstvedt (n 31) 23.

[43] Ibid.

[44] Daniel J. Solove, 'Understanding Privacy' (May 2008) GWU Legal Studies Research Paper No. 420 <https://ssrn.com/abstract=1127888> accessed on 06 October 2023.

[45] Ibid.

[46] Judith Wagner DeCew, 'The Scope of Privacy in Law and Ethics' (Aug., 1986) 5(2) Law and Philosophy 150.

[47] Charles Fried, '*Privacy [a moral analysis]*' in F. D. Schoeman (ed), *Philosophical Dimensions of Privacy* (Cambridge University Press 1984) 205.

[48] Richard A. Posner, 'The Right of Privacy' (1977) 12 Georgia Law Review 393.

perspectives challenge the traditional notion of privacy, particularly critiquing how it can perpetuate gender inequalities within the private sphere.[49]

Over time, the concept of privacy has evolved, adjusting to challenges brought by technological advancements and corporate exploitation for economic benefits or under the pretext of promoting information freedom.[50] In the current digital age, where personal data and privacy are increasingly at risk, governments face challenges in protecting data protection through legal structures and softer regulatory measures. Often, they balance privacy rights against security, economic, and other vital interests. In the digital age privacy can be harmed or infringed through surveillance, data collection, and information processing.[51] Moreover, with the rise of surveillance capitalism[52] and the rise of internet digital technologies have transformed privacy, with personal data becoming a commodity impacting on privacy, emphasizing the role of law and technology in protecting or eroding privacy rights.[53]

Privacy rights are culturally specific, and their protection, its interpretation and extent of its pursuit varies depending on a nation's or a community's cultural, economic, and political settings.[54] What is considered private and should be concealed varies from one society to another. In some societies, communal values might take precedence over individual privacy, leading to different legal and social norms regarding privacy.[55] Different countries have implemented privacy laws, revealing diverse approaches to balancing state interests and individual rights.[56]

However, ‘having deep philosophical roots and due to its vagueness and complicated scope,’ the right to privacy is very difficult to define and understand nor does it have clear legal or commonly

---

[49] Catharine A. MacKinnon, 'Feminism, Marxism, Method, and the State: Toward Feminist Jurisprudence' (1983) 08 (4) Signs: Journal of Women in Culture and Society 635.

[50] Olga Mironenko Enerstvedt (n 31) 23.

[51] Daniel Solove (n 44) 10.

[52] Shoshana Zuboff, '*The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*' (New York: Public Affair 2019) 32.

[53] Lawrence Lessig 'Privacy as Property' (Spring 2002) 69(1) Social Research 250.

[54] Kinfe Micheal Yilma (n 21) 7; Kenneth Einar Himma, 'Privacy Versus Security: Why Privacy is Not an Absolute Value or Right' (2007) 44 San Diego Law Review 904.

[55] Amitai Etzioni, 'A Communitarian Perspective on Privacy' (2000) 32 Connecticut Law Review 900.

[56] Orla Lynskey, 'The Foundations of EU Data Protection Law' (2015) Oxford University Press 90.

accepted legal definition of privacy; the process of legal formation of this right is not finalized, and privacy is 'a concept in disarray.'[57] In general, the right to privacy is continually evolving, especially with advancements in technology with multifaceted understandings of privacy balancing individual autonomy, societal interests, and technological impacts. Its nature, philosophical justifications, and criticisms are deeply rooted in the legal, social, and technological landscapes of societies.

### 2.2. Concepts and Theories on Data Protection and Right to Privacy

The relationship between data protection and privacy is complex and manifold, with areas of both convergence and divergence. Though there are traditions focusing on the variation between privacy and data protection, their connection is very close, from a theoretical, regulatory, and judicial point of view.[58] Regarding their scope, there are instances where data protection refers to the informational dimension of privacy, such as the control over information conception, the right to data protection was mainly included in the right to privacy.[59] Later, due to increased use of personal data by different actors, development of databases and technologies, it became tendency to separate the two rights, to adopt specific regulation on data protection.[60]

While privacy encompasses a broader range of considerations beyond just informational privacy, data protection specifically focuses on the handling of personal data. It can be more restrictive when considering the wide ambit of privacy but can also extend beyond traditional privacy concerns, applying to personal data processing that may not directly affect what is traditionally considered private. Activities such as the collection, storage, sharing, and transfer of passenger information can infringe on informational privacy, invoking the application of data protection standards.

Additionally, though foundational human rights documents like the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights do not explicitly define a right to data protection, they lay the groundwork for data protection laws by upholding the right

[57] Olga Mironenko Enerstvedt (n 31) 23.

[58] Ibid.

[59] Ibid.

[60] Ibid.

to privacy.[61] Some European Union instruments, however, explicitly recognize data protection as a distinct right, underscoring the intrinsic link between privacy and data protection in legislative texts.[62]

Data protection, similar to privacy encompasses various interpretations, ranging from enhancing individual control over personal information, commonly referred to as informational self-determination and the right to privacy, to perspectives centered on the free flow of information, which underscore its economic implications and the intricate interaction with privacy rights.[63] Often times, data protection is defined by procedural and legal measures that govern personal data processing, embodying a set of 'fair information practices' that operationalize the right to privacy through policy, legal, and administrative measures.

Especially, with the advent of advanced surveillance technologies, the balance between state security needs and individual privacy rights has led to the rise of understanding the link between personal privacy and personal data protection with making the latter as part of the former and at times giving it a broader scope to include rights beyond privacy.[64] Scholars have developed various theoretical frameworks to understand privacy. The relationship between data protection and privacy can be broadly categorized into three distinct perspectives.[65] The first perspective views data protection and privacy as separate yet complementary rights, recognizing their individual importance while acknowledging their interconnectedness. The second perspective posits data protection as a subset of the right to privacy, suggesting that data protection is one of the means to achieve privacy. The third perspective, however, sees data protection as an autonomous right with multiple functions, extending beyond mere privacy protection.[66] This viewpoint argues that data

[61] Ibid; Orla Lynskey (n 56) 90.

[62] Charter of Fundamental Rights of the European Union (2009) art 8; Lee Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology 251.

[63] Orla Lynskey (n 56) 91.

[64] Ibid; Alexandra Rengel, 'Privacy in International Law Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2015) 2 Groningen Journal of International Law 33.

[65] Orla Lynskey (n 56) 90.

[66] Ibid.

protection grants individuals' broader rights over a wider range of information than traditional privacy rights, particularly in the realm of personal data processing.[67]

As mentioned above, the concept of data protection can pertain to an individual's right to control their personal information.[68] It also encompasses the rights and expectations regarding the collection, storage, and dissemination of personal data, primarily addressing the questions of "what" personal information is protected and "to what extent."[69] Technically, data protection involves information technology protocols and cybersecurity measures, distinct from the legal and ethical considerations of data protection.

The third group of scholars attributes a broader aspect to data protection, defining it as encompassing economic, social, or other rights beyond ensuring the right to privacy.[70] This group also posits that effective data protection measures are crucial for ensuring privacy, with the primary difference between privacy and protection lying in their scope and focus. Data protection, as per this viewpoint, is more focused on the mechanisms and strategies to secure data from misuse.

### 2.3. International Human Right Laws Relevant for Right to Privacy

In legal terms, privacy rights are often enshrined in constitutions and human rights treaties, while data protection is detailed in specific legislation and regulations. Data protection, though not explicitly mentioned as a human right, plays a crucial role in enforcing privacy.[71] It involves technical measures like encryption, legal policies such as data breach notification laws, and organizational strategies like data minimization.

From a human rights perspective, both privacy and data protection serve to uphold the dignity and autonomy of individuals in the digital realm, integral to the dignity, autonomy, and freedom of individuals.[72] In the constantly evolving digital landscape, where vast quantities of personal and

---

[67] Ibid.

[68] Rouvroy and Poullet, 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy' (Reinventing Data Protection: Proceedings of the International Conference, Brussels, October 2007).

[69] Ibid.

[70] Orla Lynskey (n 56) 91.

[71] Ibid.

[72] GPA PSWG3 Report, 'Prepared for the GPA WG3 on Privacy and Human Rights' (2023) 43GPAPSWG3 10.

sensitive data are continuously processed, stored, and transferred, the importance of data protection has escalated. The proliferation of the internet, e-commerce, and digital communication has led to a surge in data collection, amplifying the risks and challenges in data protection.

Such a close link between privacy and data protection has also become the culture of human rights bodies when interpreting international human rights frameworks related to privacy.[73] Additionally, international human rights instruments involve provisions serving as a background for data protection. For example, the Universal Declaration of Human Rights of 1948 article 12 states, 'No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.' In a similar vein, Art 17 of the ICCPR provides, 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

Whereas the above provisions are framed in terms of a prohibition on 'interference with privacy',[74] the equivalent provisions of Art 8 of the ECHR are framed in terms of a right to 'respect for private life' it states,

> Everyone has the right to respect for his private and family life, his home and correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[73] Human Rights Council, 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development' (51st sess, agenda items 2 and 3, UN Doc A/HRC/51/42, 2022) https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf?token=TOPkuzNqYUJ2ydFKGw&fe= accessed 4 January 2024.

[74] Lee Bygrave (n 62) 251.

The other major regional human rights catalogue, the African Charter on Human and People's Rights of 1981 – omits express protection for privacy or private life.[75]

However, the Declaration of Principles on Freedom of Expression and Access to Information in Africa, adopted by the African Commission on Human and Peoples Rights, under principle 40 states that everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information including the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies.[76] It further requires states not to adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localization requirements, unless such measures are justifiable and compatible with international human rights law and standards.[77]

Additionally, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, mandates that member states enforce measures to safeguard privacy and freedom, ensuring such restrictions are essential, balanced, and in adherence to global human rights norms.[78] It also emphasizes the need to harmonize communication surveillance regulations with international human rights standards, insisting on judicial authorization and the establishment of independent oversight mechanisms. Surveillance activities should be confined to lawful, specific actions grounded in reasonable suspicion of significant criminal activity, consistent with human rights principles. The resolution advocates for the support of privacy-enhancing technologies and opposes the enactment of legislation that undermines encryption, except in instances where it can be justified under human rights law. Furthermore, it calls for the provision of remedies for individuals subjected to surveillance and the rectification of unauthorized surveillance practices.[79]

---

[75] African Court on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2019) principle 40.

[76] Ibid principle 41.

[77] Ibid.

[78] Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa - ACHPR/Res.573 (LXXVII) 2023.

[79] Ibid.

Some case law has also been developed around Art 8 of the ECHR and Art 17 of the ICCPR which indicates that both provisions embrace core data protection principles.[80] Article 17 of the ICCPR Case law developed around Art 17 of the ICCPR provides the clearest indication that the right to privacy in international law harbors core data protection principles. In its General Comment 16, the Human Rights Committee has stated that Art 17 requires legal implementation of essential data protection guarantees in both the public and private sectors.[81] In the words of the Committee:

> The competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. The gathering and holding of personal information on computers, databanks, and other devices, whether by public authorities or private individuals and bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.

For optimal protection of one's privacy, it is imperative that individuals possess the ability to understand if their personal data is being stored in automated databases, along with the specific details of such data and the purposes behind its storage.[82] Furthermore, it's crucial for individuals to know who, be it public authorities or private entities, has access to or could potentially access their information.[83] In instances where personal data is inaccurately recorded or mishandled in violation of legal standards, individuals must have the authority to demand corrections or deletions.[84]

However, the Committee only acknowledged a restriction on data collection under Article 17 but failed to emphasize the necessity of ensuring fairness in the collection process. The discussion on security measures is confined to data confidentiality, omitting the protection against unauthorized

[80] Lee Bygrave (n 62) 253.

[81] Human Rights Committee, 'General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (1988) UN Doc CCPR/C/21/Rev.1/Add.13.

[82] Ibid.

[83] Ibid para 10.

[84] Ibid.

modifications, destruction, or the prohibition of excessive data irrelevant to the processing objectives.[85]

Bygrave argues, the Committee's articulation of data protection principles is quite narrow, especially considering the extensive and detailed data protection principles available at the time of their General Comment.[86] Bygrave further notes that this raises a question about whether the Committee aimed to comprehensively outline the scope of Article 17's coverage of data protection and it could argue that the Committee, aligning with traditional views of privacy as a form of seclusion, intentionally focused its guidelines on protecting individuals' rights to keep their information private.[87]

### 2.4 Rise of Surveillance Technology and Balancing Interests

Surveillance, as a concept and practice, has a long history, tracing back to ancient times with spies in early empires and evolving through various forms such as the panopticon in the 18th century.[88] The 20th century marked a significant turning point with the advent of electronic and digital surveillance technologies, radically changing the landscape of surveillance capabilities.

In an era where technological advancements are rapid and pervasive, the challenge of regulating data protection has intensified significantly. This escalation is largely due to the emergence and continuous evolution of various technological phenomena, such as the widespread use of big data, the increasing sophistication of artificial intelligence, and the proliferation of the Internet of Things.[89] These developments continually test the resilience and adaptability of existing data protection frameworks, highlighting their limitations and the need for ongoing revision.

---

[85] Ibid para 8.

[86] Lee Bygrave (n 62) 253.

[87] Ibid.

[88] Susan Flynn and Antonia Mackay, 'Surveillance and Spatial Performativity in the Scenography of Tower Lucy Thornett in' (2019) Palgrave Macmillan 80; Matthew Alen, 'Convict Surveillance and Reform in Theory and Practice, Jeremy Bentham vs New South Wales' (2022) 3.

[89] Jordanco Sekulovski, 'The Panopticon Factor: Privacy and Surveillance in the Digital Age' (2016) Project Innovative Ethics 20.

One of the most complex aspects of this challenge is the inherently international nature of data flow, which raises critical questions regarding jurisdiction and the enforcement of laws across borders.[90] This situation demands a delicate balancing act between national interests, which include both security concerns and economic imperatives, and the rights to individual privacy, a balance that remains a source of significant debate and contention.[91]

The increased focus on global terrorism, coupled with advancements in technology and expanded government surveillance, has sparked a broad and ongoing debate.[92] This debate centers on the nature and extent of surveillance, its implications, and the ethical considerations it raises.

From a philosophical perspective, the debate between surveillance and human rights, particularly the right to privacy often hinges on utilitarian principles defending national security, which advocate for the greatest good for the greatest number.[93] This perspective suggests that stringent security measures are justified if they protect the majority, even at the cost of individual privacy.

The liberal tradition, with its emphasis on individual rights and freedoms, is a strong proponent of privacy.[94] However, the rights to privacy are deeply rooted in liberal philosophy, which values individual liberty and autonomy.[95] This school of thought warns against compromising privacy, as it could lead to an Orwellian society where individual freedoms are severely undermined. Post-World War II, the establishment of the United Nations and the Universal Declaration of Human Rights marked a global recognition of individual rights.[96]

---

[90] OECD, 'Mapping Approaches to Data and Data Flows' (2020) Report for the G20 Digital Taskforce, OECD Publishing 6.

[91] Ibid.

[92] UNCTAD, 'Data protection regulations and international data flows: Implications for trade and development' (2016) 15.

[93] Dembi, Divyanshu, 'Privacy & National Security: A Balancing Act?' (January 30, 2021) <https://ssrn.com/abstract=3953357>or< http://dx.doi.org/10.2139/ssrn.3953357> accessed 17 January 2024.

[94] Matthew Alen (n 88) 3.

[95] Robert B. Hallborg, Jr, 'Principles of Liberty and the Right to Privacy' (1986) 5(2) Law and Philosophy 180.

[96] Ibid 9.

In contrast, the communitarian perspective advocates for a more balanced approach, taking into account the safety and responsibilities of the community as a whole.[97] Michel Foucault's concept of panopticism describes a society where constant surveillance leads to a form of self-regulation among individuals.[98] Additionally, ethical debates revolve around the justification of surveillance for security purposes versus its potential for abuse and the infringement on individual rights.[99] The rapid development of technologies, such as facial recognition and AI, introduces new ethical dilemmas and privacy concerns, especially considering the vast amounts of personal data that are now collected, stored, and processed.[100]

In the realm of mass surveillance, technologies such as drones, biometric surveillance, and data mining have played pivotal roles. The use of AI in processing surveillance data presents a paradox of opportunities and challenges for privacy protection.[101] Issues such as bias and discrimination in predictive policing, and the looming threat of a surveillance state, are at the forefront of current discourse.[102] This has led to increasing calls for the establishment of global norms and regulations for data protection and surveillance.

The most direct impact of surveillance technologies is on privacy, where infringements occur through unauthorized data collection, monitoring communications, and tracking individual movements.[103] Surveillance can lead to self-censorship, impeding free expression and the right to

---

[97] Etzioni, Amitai, 'A Communitarian Perspective on Privacy' (2000) 32(3) Connecticut Law Review. <https://ssrn.com/abstract=2157015> accessed on 26 January 2024.

[98] Matthew Alen (n 88) 3.

[99] Etzioni, Amitai (n 97) 10.

[100] Denise Almeida, Konstantin Shmarko, and Elizabeth Lomas, 'The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks' (2022) 2 AI and Ethics 377.

[101] Gai Sher and Ariela Benchlouch, 'The privacy paradox with AI' *Reuters* (Toronto, October 2023) <https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/> accessed 03 February 2024.

[102] Kristian Lum, 'Predictive Policing Reinforces Police Bias' (October, 2016) Human Rights Data Analysis Group <https://hrdag.org/2016/10/10/predictive-policing-reinforces-police-bias/> accessed 03 February 2024.

[103] Daniel J. Power, Ciara Heavin, Yvonne O'Connor, 'Balancing privacy rights and surveillance analytics: a decision process guide' (2021) 4(2) Journal of Business Analytics 30.

associate. Data and evidence gathered through surveillance sometimes can be used in legal proceedings without adequate oversight or transparency.[104]

The Cold War era's espionage, ideological battles, and events like the September 11, 2001, terrorist attacks marked a significant shift, with governments worldwide (especially developed nations such as US) enacting laws that expanded surveillance capabilities, often at the expense of privacy rights.[105] This has led to increased state surveillance, frequently justified by national security concerns.[106] In this context, both in authoritarian states and democracies, surveillance is often utilized as a tool of political power, significantly impinging on human rights.[107] Therefore, ensuring government transparency and accountability in surveillance activities, encouraging active public engagement in policymaking, and implementing robust privacy-enhancing technologies are considered crucial steps towards achieving a more balanced outcome and safeguarding individual data.

Accordingly, the control over the collection and dissemination of personal information has become increasingly relevant in the digital age where data collection and surveillance are pervasive. This also entails the safeguarding of the confidentiality of personal communications, including letters, emails, and phone calls. [108] This is important for so many reasons. Firstly, philosophically speaking, privacy is seen as essential for personal autonomy and dignity.[109] It allows individuals to think, experiment, and make decisions independently, free from external scrutiny or interference. Moreover, privacy is linked to liberty, especially in terms of freedom of thought and expression. It provides a space for individuals to explore ideas without fear of public judgment or censorship.[110] Thirdly, protection of privacy promotes democracy and pluralism where in democratic societies, privacy is crucial for ensuring a pluralistic society where diverse opinions

[104] Ibid.

[105] Kenneth Einar Himma, 'Privacy Versus Security: Why Privacy is Not an Absolute Value or Right' (2007) 44(1) San Diego Law Review 865.

[106] Ibid 870.

[107] Ibid.

[108] Valerie Steves, 'Now You See Me: Privacy, technology and Autonomy in the Digital Age' (2023) University of Ottawa 10.

[109] Ibid.

[110] Ibid.

and lifestyles can flourish without fear of persecution or conformist pressures.[111] Additionally, privacy entails psychological justifications in which privacy is considered as necessary for emotional and mental well-being, offering individuals a respite from the public gaze and a space for intimate relationships and personal growth.[112]

Despite issues of national security and public interest, the need for the protection of personal privacy irrespective of whichever justifications associated to its infringement is crucial. This can be realized in different ways such as in the context of national security, the need for proportionality and strict oversight is emphasized to balance security interests with privacy rights.[113] Furthermore, advocates stress the importance of informed consent and transparency in data collection and use, advocating for robust data protection laws. adapting legal frameworks needs to be emphasized to keep pace with technological advancements, ensuring that privacy protections remain relevant.[114]

[111]Carissa Véliz, 'Democracy, Politics, Privacy and Surveillance' (6 April 2021) https://www.bostonreview.net/articles/why-democracy-needs-privacy/.

[112] Charles Fried, 'Privacy' (1968) 77(3) Yale Law Journal 480.

[113] Olga Mironenko Enerstvedt (n 31) 25.

[114] Ibid.

## Chapter Three

### 3. Surveillance Practices and Current Legal regime in Ethiopia

### 3.1. General Overview of Ethiopia's Privacy and Data Protection Legal Framework

Ethiopia's legal framework for privacy and data protection is in its early stages. There's a belief among some scholars that Ethiopian culture's emphasis on communal and social values has historically overshadowed the concept of individual privacy.[115] Nonetheless, Ethiopian authorities have, over time, enacted various laws aimed at safeguarding individuals' privacy and property from unauthorized interference, with the level of protection fluctuating across different periods.[116] Notable instances include the constitutional enactments of 1931, 1955, and 1987. The 1931 Constitution, along with its 1955 revision, explicitly safeguarded Ethiopian citizens' rights against unwarranted home searches and ensured the confidentiality of their correspondence, excepting legally justified exceptions.[117] Similarly, the 1987 Constitution, promulgated during the Derg regime, affirmed the sanctity of Ethiopians' personal and domestic privacy and the confidentiality of their communications. Although the interim government's Charter did not directly address privacy rights, it pledged full adherence to the UDHR, which encompasses Article 12 on the right to privacy.[118]

Ethiopia is also a signatory to major global human rights treaties, such as the ICCPR among others. These agreements delineate various fundamental rights, such as the right to privacy, personal security, freedom of movement, and freedoms of opinion, expression, and association.[119]

Specifically, Article 17 of the ICCPR mandates that no individual should suffer arbitrary or unlawful interference with their privacy, family, home, or communications, ensuring legal protection against such infringements. In 2019 the UN Human Rights Council, declared that individuals' rights must be preserved both online and offline, with the understanding that these

[115] Kinfe Michael Yilma (n 21) 3.

[116] Ibid.

[117] The Revised Constitution of Ethiopia, 1955, art 61.

[118] Kinfe Michael Yilma (n 21) 3.

[119] ICCPR, arts 17, 9, 12, 19, 21, 22; ACHPR, arts 5, 6, 12, 9, 10, 11.

rights are not absolute, and any restrictions must adhere to international legal standards, including lawfulness, necessity, proportionality, and specificity.[120]

Furthermore, limitations on privacy must be legally justified, aiming for a legitimate purpose, and be both necessary and proportionate to that end.[121] The UN special rapporteur on freedom of expression has emphasized the intrusive nature of communication surveillance, advocating that it be conducted only under exceptional circumstances, supervised by an independent judicial body, and within the bounds of clearly defined legal parameters.[122]

Apart from the above mentioned international human rights instruments in which Ethiopia considers as part of its law[123], the right to privacy is firmly anchored in the Constitution.[124] Article 26 of the Constitution guarantees comprehensive privacy rights, including protection against unwarranted searches of homes, persons, or property, and the seizure of personal possessions. It also safeguards the inviolability of personal communications, including postal letters and electronic communications.[125]

These provisions obligate public officials and the government to uphold these rights, except under exceptional circumstances that justify infringement, such as national security, public peace, crime prevention, health, public morality, or the protection of others' rights and freedoms.[126] These exceptions must align with specific laws.[127] Although the Constitution primarily addresses public officials, it also implies obligations for other entities, including corporations, to respect privacy rights.

---

[120] Human Rights Council, 'Right to privacy, Report of the Special Rapporteur on the right to privacy' A/HRC/40/63, 2019.

[121] Ibid.

[122] Ibid.

[123] Constitution of the Federal Democratic Republic of Ethiopia (1995), art 9/4.

[124] Ibid art 25.

[125] Ibid art 26.

[126] Ibid.

[127] Ibid.

### 3.2. Key Domestic Laws Governing Personal Data Protection in Ethiopia

Before Ethiopia's comprehensive Personal Data Protection Law came into effect, data protection rules and provisions were dispersed across various pieces of legislation. This piecemeal approach included laws such as the Civil Code,[128] the Criminal Code,[129] Telecom Fraud Proclamation No. 761/2012,[130] Computer Crimes Proclamation No. 958/2016,[131] Freedom of Mass Media and Access to Information Proclamation No. 590/2008,[132] Federal Income Tax Proclamation No. 979/2016,[133] Electronic Signature Proclamation No. 1072/2018,[134] and Financial Consumer Protection Directive No. FCP/01/2020.[135]

These laws collectively cover a broad spectrum of data protection concerns. For instance, the Civil Code includes provisions that recognize privacy rights including the protection of individual domiciles.[136] Some laws impose obligation on data controllers from unauthorized access and data breaches protecting the data privacy of data subjects.[137] For example the telecom fraud proclamation protects data of telecom service subscribers from illegal interception, access, alteration, destruction, or damage.[138] Additionally, the Computer Crimes Proclamation No. 958/2016 protects all types of data on computer systems from unauthorized and illegal access, interception, and damage as well as has provisions dealing with identity theft, computer related forgery and fraud. The Computer Crimes Proclamation also has a clause on the "right to be forgotten" and other important data protection principles including data minimization and lawfulness of data processing.[139] However, this law is also criticized for being detrimental for data

[128] The Civil Code of the Empire of Ethiopia 1960, arts 11, 12, and 13.

[129] The Ethiopian Federal Democratic Republic Criminal Code 2000, arts 604, 606.

[130] Telecom Fraud Proclamation No.761/2012.

[131] Proclamation to Provide for the Computer Crime Proclamation No 958/2016.

[132] Freedom of Mass Media and Access to Information Proclamation No. 590/2008.

[133] Federal Income Tax Proclamation No. 979/2016.

[134] Electronic Signature Proclamation No. 1072/2018.

[135] Financial Consumer Protection Directive No. FCP/01/2020.

[136] The Civil Code of the Empire of Ethiopia 1960, arts 11-13.

[137] The African Declaration (n 74) 28; See for example the Financial Consumer Protection Directive No. FCP/01/2020, art 5/4.

[138] Telecom Fraud Proclamation No.761/2012, art 5/3.

[139] Proclamation to Provide for the Computer Crime Proclamation No 958/2016, arts 24, 3, 4, 5, and 6.

subjects' rights and for failing to incorporate some necessary principles on data protection.[140] It in particular allows service providers to retain data traffic for one year and must keep it confidential, without providing an obligation to disclose this to the data subject.[141] Thus, limiting the data subject's right to participate and be informed in the handling of his personal data.

Other significant legislation includes the Vital Events Registration and National Identification Card Proclamations. The law stipulated agencies entrusted to enforce these laws, making them responsible to collect data including sensitive data (aka special categories data) including the identity, religion and ethnicity of data subjects.[142] Although these laws incorporate principles like confidentiality and data quality, their implementation does not always strictly adhere to data protection rights, which may jeopardize data subjects' rights. The National Identification Card Proclamation, for instance, holds anyone whether private or public sector responsible for damaging, destroying, suppressing, or unlawfully accessing data collected in relation to registration of vital events and ID card issuance. However, the vital events registration law and the National ID card proclamation, by allowing storage of data for other unspecified purposes seems to contravene the purpose limitation principle.[143]

The Freedom of Mass Media and Access to Information Proclamation No. 590/2008, is another broad law that includes data protection clauses. This law provides a broad definition to what personal information means, encompassing a range of categories including medical, educational, employment, and financial histories; demographic details like ethnic, national, or social origins, age, and marital status; personal identifiers such as addresses and fingerprints; and personal opinions and preferences, with certain exclusions.[144] It also recognizes the requirements of informed consent, data transfer, and the right to be forgotten.[145]

The Financial Consumer Protection Directive No. FCP/01/2020 obliges financial service providers to implement policies and procedures that protect financial consumers' data including

[140] The African Declaration (n 71) 28.

[141] Proclamation to Provide for the Computer Crime Proclamation No 958/2016, art 24.

[142] Ibid arts 24, 30, 34 and etc.

[143] Ibid art 64/5.

[144] Freedom of Mass Media and Access to Information Proclamation No. 590/2008, art 2/8.

[145] Ibid art 20.

the collection, usage, disclosure and the identity of the data.[146] According to this law data refers to any information regarding an identified or identifiable financial consumer (a current or prospective client of a financial service provider) or security provider.[147] These providers are expected to maintain the confidentiality and security of all customer data, and their policies to be transparent, accessible on bank websites and available upon customer request.[148] It also requires lawful and fair data collection for legitimate purposes, adherence to confidentiality by third parties receiving such data, and provisions for customers to access and correct their data, upholding the Security Safeguards and Individual Participation Principles.[149]

There are other laws governing data protection related rights and issues including the Federal Income tax Proclamation no. 979/2016 and the Electronic Signature Proclamation no. 1072/2018[150], however, detailed exploration of these laws will be beyond the scope of the study.

### 3.3. Introduction to Surveillance Practices in Ethiopia and Impact on Human Rights

Surveillance in Ethiopia, deeply intertwined with the nation's political evolution, traces back to the oppressive Derg regime and continued under the Ethiopian People's Revolutionary Democratic Front.[151] These historical surveillance practices targeted political opponents, including politicians, scholars, and journalists, stifling broader political and public engagement.[152] With technological advancements, the government's surveillance capabilities have significantly expanded,[153] facilitated by the control over telecommunications through entities like Ethio Telecom. This has led to unauthorized surveillance, interceptions of communications, and a culture of self-censorship detrimental to free discourse and political dissent.[154]

---

[146] Financial Consumer Protection Directive No. FCP/01/2020, Preamble.

[147] Ibid art 2/2 (6).

[148] Ibid arts 4/2 and 4/4.

[149] Ibid.

[150] Electronic Signature Proclamation No. 1072/2018, art 29. This article obliges any certificate provider to keep custody of any information related to certificate issuance, suspension, revocation, or related services for 2 years and to keep personal information confidential.

[151] Kinfe Michael Yilma (n 21) 3.

[152] Saskia Brechenmacher (n 14) 66.

[153] Ibid 67.

[154] Human Rights Watch (n 14).

The expansion of telecommunications infrastructure has been both a boon and a bane; it has enhanced connectivity and information exchange, but also served as a tool for suppression.[155] Advanced technologies have been integrated into state surveillance operations, notably during periods of political unrest, with the government importing sophisticated technology for in-depth monitoring.[156] This has raised severe privacy and press freedom concerns, as vigilance over platforms like Facebook has led to arrests over dissenting views, and internet shutdowns have curtailed fundamental rights such as access to information, education, and healthcare.[157]

While the government asserts that these surveillance measures as crucial components of its national security and anti-terrorism initiatives, underpinned by various laws and regulations aimed at safeguarding national stability, they have severely impacted civil liberties, leading to politically motivated prosecutions and a stifling of independent media and civil society. [158] A significant incident in this context occurred in February 2014 when the Electronic Foundation took legal action against the Federal Democratic Republic of Ethiopia on behalf of Mr. Kidane, an Ethiopian-born U.S. citizen. His computer in Maryland was compromised with FinSpy malware, usually restricted to state and law enforcement use, allowing the Ethiopian government to intrude on his digital privacy illegally.[159]

Reports suggest that surveillance targets are not always selected based on legitimate security threats, and the methods employed are often unlawful.[160] The authorities' surveillance efforts disproportionately focus on individuals associated with opposition groups, journalists, or certain religious affiliations, regardless of actual security risks. This broad targeting, sometimes based on

---

[155] Daniel Grinberg, 'Chilling Developments: Digital Access, Surveillance, and the Authoritarian Dilemma in Ethiopia, Surveillance and Society' (2017) 15 Surveillance & Society 432.

[156] Ibid.

[157] Ibid 435.

[158] Ibid.

[159] Kidane v Government of Ethiopia [2016] USCA DC 16-7081 (Court of Appeals, DC Circuit) https://www.cadc.uscourts.gov/internet/opinions.nsf/E0C614D73F037CAD852580E3004EE648/$file/16-7081-1665840.pdf. The court held that, because the Ethiopian government hatched its plan in Ethiopia and its agents launched the attack that occurred in Maryland from outside the U.S., the Foreign Sovereign Immunities Act (FSIA) prevented U.S. courts from even hearing the case.

[160] Daniel Grinberg (n 155) 435.

ethnicity, lawful activities, or familial ties, undermines the potential of technology to enhance freedoms of expression, information access, and association.

The pervasive fear and reality of surveillance have led many, including journalists, politicians, and academics, to self-censor their communications.[161] This climate of fear not only limits personal freedoms but also diminishes the societal benefits of open and free communication.

The legal frameworks in place, such as the Proclamation to Prevent Terrorism and the Computer Crime Proclamation, provide the government expansive surveillance powers. These laws allow for practices like phone tapping, data analysis, and the use of surveillance tools against perceived political threats, often blurring the lines between national security and political suppression. For instance, Article 31 of the Prevention and Suppression of Terrorism Crimes Proclamation allows police to conduct surprise searches to prevent terrorism offenses, relying solely on permission from a high-ranking police official. While this provision aims to enable rapid responses to prevent potential terrorist acts, it opens the door to arbitrary searches and seizures. The procedural safeguard of requiring a police officer to prepare a list of seized property and secure signatures from either the suspect or a neutral witness introduces a measure of accountability.[162] However, the absence of immediate judicial review is a significant concern, as it increases the potential for abuses of power and violations of privacy and property rights.

Under Article 34 of the same proclamation, the police are permitted to compel individuals and entities to furnish information that could assist in preventing or investigating terrorism. Normally, this requires a court order; however, in ‘urgent cases,’ this judicial prerequisite can be bypassed, with the police required to seek retroactive court approval within 72 hours.[163] This article's lack of clarity on what constitutes an 'urgent case' coupled with the reliance on post facto judicial review could lead to preemptive and possibly unwarranted breaches of privacy. The police's substantial discretionary power in determining ‘urgency’ raises significant concerns about subjective judgment and potential misuse. Furthermore, it doesn’t provide sufficient mechanisms to safeguard the information collected during the 72-hour window period if the court rejects the police’s request.

[161] Human Rights Watch (n 14).

[162] Prevention and Suppression of Terrorism Crimes Proclamation No. 1176/2020, art 31/2.

[163] Ibid art 34/2.

Moreover, absence of clear guidelines on the admissibility of such evidence or on the procedures for its disposal further undermines protections against arbitrary privacy interference.

Article 42 of the same proclamation permits the use of advanced surveillance techniques, including intercepting communications and employing undercover agents, provided there is court authorization or, in urgent situations, approval from a public prosecutor, with subsequent court validation required within 48 hours. Although this article attempts to mitigate risks by mandating eventual court oversight, the initial lack of judicial review could present considerable risks to personal privacy and data protection.

Article 43 of the same proclamation obliges any person to provide information that may assist the police to prevent terrorist attack or investigation to the police. This broad directive, without court oversight, could lead to excessive collection of personal data under the guise of national security. Furthermore, the fact that the determination of what constitutes 'defamatory to the suspects' privacy right' seems to be left to police discretion,[164] potentially leading to excessive data collection and unwarranted surveillance without adequate judicial oversight. Although sub-Article 4 introduces measures to safeguard the privacy of suspects—requiring the police to keep the obtained information confidential and use it solely for specified objectives—this protection is conditional. The determination of whether the collected information qualifies as 'secret' remains at the discretion of the police. This grants excessive power to the police and leaves data subjects vulnerable to potential privacy violations.

Another key law is the Proclamation to Provide for Computer Crime Proclamation No 958/2016 that empowers various governmental bodies to actively monitor and intervene in computer-related activities. Article 25(3) of the Proclamation permits the Attorney General to authorize investigatory organs to conduct surveillance without a court warrant in cases deemed urgent, where there are reasonable grounds to believe a computer crime threatening critical infrastructure is imminent. However, the Attorney General must present the reasons for this surveillance to the President of the Federal High Court within 48 hours, awaiting the court's decision[165]. This provision raises significant privacy concerns, particularly in the scenario where the court might

[164] Ibid art 43/2.

[165] Proclamation to Provide for the Computer Crime Proclamation No 958/2016, art 25/4.

decline the surveillance request after the 48-hour period. The fate of data collected during this window is not explicitly addressed in the proclamation, creating a legal ambiguity that could lead to the retention and use of potentially unlawfully obtained evidence. Furthermore, Article 32 (2) allows investigatory organs to extend searches or access to additional computer systems without a separate search warrant if they believe the sought data is stored on or obtainable through another system, giving broad powers that could lead to expansive searches.

Article 27 of the same proclamation mandates service providers to report knowledge of any crimes or illegal content dissemination through their systems. The broad definition of 'content data' under Article 2 of the proclamation includes any form of communicative data, potentially subjecting data subjects to extensive surveillance and reporting by service providers. This requirement could pressure service providers to monitor user data closely,[166] potentially leading to over-surveillance and infringing on privacy rights. This mandatory cooperation can further lead to ethical dilemmas and conflicts between protecting user privacy and complying with legal obligations, potentially turning service providers into de facto agents of state surveillance.

The Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation is another law that accords surveillance powers to the Police. Article 25 of the Proclamation details specific investigative techniques that can be authorized by the judiciary to gather evidence of money laundering or terrorism financing and to trace criminal proceeds. These techniques include monitoring bank and similar accounts, accessing computer systems, networks, and servers, placing individuals under surveillance, or intercepting their communications, taking audio or video recordings of acts, behaviors, and conversations, and intercepting and seizing correspondence. These methods are permissible only when there are serious indications that the targeted systems or accounts are being used by individuals suspected of engaging in these illegal activities.[167] The use of these techniques is conditioned on obtaining judicial authorization and is limited to a defined period to ensure the measures are both necessary and proportionate to the suspicions at hand. However, the broad and invasive nature of these authorized powers still poses a substantial risk of

[166] Kinfe Michael Yilma (n 25) 453.

[167] Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No 780/2013, art 25(2).

abuse, which could lead to rights violations and diminish public trust in law enforcement and judicial systems.

The Telecom Fraud Offense Proclamation also permits the police to request a covert search warrant from the court if a telecom fraud offense has occurred or there is reasonable suspicion that such a fraud is likely to occur.[168] This provision allows for preemptive and responsive measures in the investigation of telecom-related crimes. However, this raises concerns about the potential for overreach and privacy violations, particularly if the criteria for "reasonable grounds" are not clearly defined or are too broadly interpreted.

Furthermore, organizations like the Information Network Security Agency (INSA) and National Intelligence Service (NIS) are also empowered with an extensive power of surveillance through their establishment proclamations and other laws. Article 8/7 of the NIS establishment proclamation for instance allows the NIS to conduct surveillance upon obtaining a court warrant. This provision introduces a crucial layer of judicial oversight, which is vital for protecting individual rights against unwarranted intrusions. Comparatively, INSA's establishment proclamation authorized to conduct digital forensic investigations remotely without a court warrant, especially on computers or infrastructures identified as potential sources of cyberattacks.[169] This power, while crucial for cybersecurity, allows for profound privacy intrusions without adequate judicial review.

Article 27 of NIS's establishment proclamation obliges individuals to cooperate with the NIS by providing intelligence or evidence. However, this requirement lacks an independent review mechanism, creating room for potentially excessive intrusions into personal data. Similarly, the INSA establishment proclamation stipulates a similar duty to cooperate provision in its operations to prevent and investigate cybercrimes and lacks clarity on privacy safeguards, which could lead to undue breaches of privacy.[170] Moreover, Article 11 of the Council of Ministers Regulation to Provide for Execution of Information Network Security Agency Reestablishment Proclamation, Regulation No. 320/2014, stipulates that INSA is not required to reveal its information sources or

[168] Telecom Fraud Offense Proclamation No. 780/2013, art 14.

[169] Information Network Security Agency Re-establishment Proclamation No. 808/2013, art 6/8.

[170] Ibid art 12.

collection methods even to courts. This opacity can undermine the accountability necessary for such powerful surveillance capabilities.

The Ethiopian Communication Service Proclamation grants the Ethiopian Communications Authority (ECA) extensive powers to ensure compliance with its regulations, including the ability to assign inspectors to enter and inspect premises, access telecommunications equipment, and examine documents.[171] Telecommunications operators are obliged to maintain customer confidentiality yet must comply with court orders to provide customer data and facilitate lawful government surveillance for criminal or national security investigations.[172] These operators are also required to register all SIM cards and contribute to a National Subscriber Registry to aid in national security efforts.[173] While these measures are designed to balance national security with operational integrity, they raise concerns about potential overreach and the impact on individual privacy. Thus, there is a need for stringent safeguards and clear guidelines on compliance and judicial oversight.

Ethiopia's balancing act between security needs and individual freedoms reveals a complex legal landscape where national security imperatives often overshadow privacy rights. The expansive surveillance powers granted through various laws, such as the Proclamation to Prevent Terrorism and the Computer Crime Proclamation, allow significant state oversight under the guise of national security. These laws empower authorities like the Police, NIS, and INSA to conduct broad surveillance activities, often without immediate judicial review, which poses significant risks to personal privacy and civil liberties. Furthermore, mandatory cooperation requirements exacerbate these challenges, potentially turning service providers into extensions of state surveillance mechanisms. While certain safeguards like *ex-ante* and *post-facto* judicial approvals and procedural checks are in place, they often fall short of providing real-time protections against privacy infringements.

However, with the introduction of the new Personal Data Protection Proclamation which provides a comprehensive framework, some of the surveillance challenges highlighted above can be

[171] Communication Service Proclamation No. 1148/2019, art 31/1.

[172] Ibid art 51.

[173] Ibid art 51/4.

addressed. This is mainly because the new law provides a comprehensive protection framework with an effective authority over other personal data related laws and practices.[174]

According to Article 68 of the PDPP, personal and sensitive personal data collected before the PDPP takes effect must be processed according to the Proclamation's standards, regardless of the rules under which they were collected. This retroactive effect of the PDPP gives a crucial opportunity for creating a unified standard to personal data protection and to ensure all personal data, regardless of when it was collected to be treated under the stringent protection standards set by the PDPP. This will also lead to the reevaluation of existing legal and operational frameworks in both private and public sectors, forcing them to align their data-handling practices with the PDPP's stricter and perhaps more comprehensive personal data protection requirements.

Furthermore, article 67 of the PDPP provides that any laws or practices inconsistent with the PDPP will not apply to matters covered by the Proclamation. This supremacy plays a critical role in shaping personal data protection practices particularly surveillance practices in the country. Firstly, it obliges the revision of personal data handling practices including data collection, processing, storing, and accessing practices that are against the principles enshrined under article 6 and the following provisions of the PDPP. Thus, creating the opportunity for any laws and procedures that give rise to surveillance to be interpreted and implemented in a strict adherence of the principles of the PDPP. Secondly, by forcing both the public and private sectors to adopt stringent data protection measures and accountability framework, it can reshape the existing surveillance practices towards a more responsible surveillance practice. Consequently, limiting the extensive surveillance power accorded to security and law enforcement agencies in various legislations.

### 3.4. The Personal Data Protection Proclamation No. 1321

In the contemporary digital era, the protection of personal data is a paramount concern. Recognizing this imperative, Ethiopia has enacted a Personal Data Protection Proclamation, a comprehensive legislative framework designed to safeguard personal data.[175] The PDPP is crafted to uphold the right to privacy for individuals, safeguarding them against unauthorized access or breaches of their personal data.[176] This framework regulates the usage of personal data in profiling

[174] Ibid arts 67 and 78.

[175] Personal Data Protection Proclamation No. 1321 2024 (herein after PDPP).

[176] Ibid arts 2 and 3.

activities and mandates the use of pseudonymization techniques to ensure that individuals cannot be directly identified from the data.[177] The law is applicable to both automated and non-automated processes of handling personal data. It is relevant to data controllers or processors operating within Ethiopia, as well as those utilizing equipment in the country, unless the data is only in transit.[178]

For data controllers or processors not physically located in Ethiopia but processing data that originates from or involves the use of Ethiopian equipment, the law requires the appointment of a local representative.[179] This representative must meet certain criteria, such as residency in Ethiopia.[180]

The PDPP does not explicitly specify whether its provisions apply to private, public institutions, or both. However, a thorough analysis of its provisions suggests that it imposes equal obligations on both sectors. Unlike the sector-based data protection rules common in the US the PDPP attempts to govern all sectors and entities whether public or private or financial or non-financial sectors.[181]

The PDPP includes certain conditions in which public authorities may be exempted from standard data processing regulations.[182] These exceptions apply when necessary for national security, defense, public safety, criminal investigations and prosecutions, objectives of national interest (including the state's economic or financial interests), maintaining judicial independence, or safeguarding the rights of the data subject or others.[183] Violations of these exemptions permit the data subject or the Authority to seek legal remedies to protect individual rights.[184] Furthermore, article 7/2/f stipulates that data processing is permissible if it serves the legitimate interests of the data controller or a third party, unless these interests are outweighed by the fundamental rights and freedoms of the data subject that necessitate data protection.[185] This article aims at balancing the

[177] Ibid arts 2/22 and 17/4.

[178] Ibid art 3.

[179] Ibid.

[180] Ibid.

[181] The explanatory note of the PDPP 3.

[182] PDPP arts 53 and 54.

[183] Ibid.

[184] Ibid art 53/3.

[185] Ibid arts 53 cum 7/2/e and f.

rights of data subjects and the processing rights of third parties which are usually in conflict. However, it should be understood in relation to the consent of the data subject securing of which may hamper the right of the third parties from processing or accessing it.

The new law defines key terms such as personal data, data subject, data controller, and data processor in a manner like other data protection regimes including the European Union General Data Protection Regulation (GDPR). Personal data is defined as any information related to an identified or identifiable natural person, including opinions about the individual and intentions of the data controller or others towards them.[186] Sensitive personal data, which includes information about racial or ethnic origins, genetic and biometric data, health conditions, sexual life, political opinions, religious beliefs, trade union membership, criminal offenses, and other categories determined by the Commission, is given special consideration.[187] Moreover, consent is defined as a freely given, specific, informed, and unambiguous indication of a data subject's wishes, signified by either a statement or a clear affirmative action, agreeing to the processing of their personal data.[188]

Article 7/1 inclines to take the position of prohibitive as it prohibits processing, 'personal data shall not be processed unless there is compliance with at least one of the conditions set out in sub articles (2) and (3); or in the case of sensitive personal data, article 9.'[189] Though such a provision, according to some authors is considered detrimental to data flow such safeguards can be interpreted as better safeguarding conditions for privacy rights,[190] the quality of data protection if it means to safeguard privacy rights should be coined in such a way.[191]

### 3.4.1. Principles of the New Personal Data Protection Proclamation

The PDPP's principles are crafted, covering a wide spectrum of data protection aspects from lawfulness to data subject rights. Most principles in the PDPP align with the GDPR and even the

[186] Ibid art 2/17.

[187] Ibid art 2/26.

[188] Ibid art 2/5.

[189] Ibid art 16/1.

[190] Orla Lynskey (n 56) 60

[191] Ibid.

OECD principles that could indicate the capacity and commitment to upholding high data protection standards by Ethiopia.[192]

#### 3.4.1.1. Principle of Lawfulness or Legality

The legality principle is closely related to the concepts of legal formalism and the rule of law that implies that states and their institutions such as the law enforcement agencies must observe the rule of law, whereby all acts of law enforcement agencies have to comply with the law and such acts cannot be carried out outside the limits and boundaries delineated by the law.[193] Accordingly, the law must be clear, ascertainable and no law must be given retroactive effect. Hence, decision makers must apply legal rules that have been declared beforehand, and not alter the legal situation retrospectively by discretionary departures from established law. The principle of lawfulness in the context of personal data processing is a fundamental aspect of data protection regulations. The criteria that, 'personal data shall be processed lawfully, fairly and in a transparent manner law' implies, first, that any limitation, any interference must have a legal basis. No security measure that interferes with human rights can be adopted in the absence of an existing publicly available legislative act.[194] Moreover, the processing should be made in a transparent way where clarity and accessibility of data processing should be ensured.

The principle of legality also ensures that personal data is processed legally, underpinning the entire framework of data processing activities. It serves as a bedrock, providing a legal basis and set guidelines that must be adhered to ensure the protection of individuals' privacy and personal data. The principle strikes a balance between the need for data processing in various contexts and the protection of individual rights, emphasizing the importance of consent, the necessity for processing, and the protection of sensitive data.[195] At the core of this principle is the requirement that personal data must be processed under specific predetermined conditions.

---

[192] See the Organization for Economic Cooperation and Development, Decision of the Secretary-General on the Protection of Individuals with regard to the Processing of their Personal Data, art 4; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR).

[193] Olga Mironenko Enerstvedt (n 31) 168.

[194] Ibid.

[195] PDPP art 7/2 (a).

One of the critical aspects of this principle is the requirement for the data subject's consent. Consent must be obtained before any processing activity,[196] ensuring that individuals have control over their personal data. A valid consent must be freely given, informed, specific, clear, and capable of being withdrawn.[197] This law not only obliges the data controller to refrain from misrepresentation and confusion but also to process the data based on the consent given with regard to processing of specific data for a specified purpose prohibiting the data controller from processing and shall not make the provision of any goods or services or the quality thereof, the performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purposes.[198]

Once given, the withdrawal of consent does not retroactively affect the legality of any processing carried out prior to the withdrawal.[199] However, this aspect of the PDPP is critiqued for potentially making the withdrawal process more cumbersome than giving consent.[200]

In the absence of consent, processing is only permissible if it is necessary for the execution or preparation of a contract with the data subject, if it is necessary for compliance with the legal obligation of data controller (such as tax obligations), to protect the vitally important interests of the data subject or protect the legitimate interests of the data controller.[201] However, this privilege should be construed narrowly to ensure a fair balance between the interests of data controllers and the rights of data subjects as well as between the rights of individuals and the necessity of data processing in various contexts.

In situations of national emergencies, public order, and safety, the principle allows for the processing of personal data as a necessity.[202] This extends to scenarios where data processing is

---

[196] Ibid art 8/1.

[197] Ibid art 8/2.

[198] Ibid art 8/4.

[199] Ibid art 8/6.

[200] Center for the Advancement of Rights and Democracy, Position Paper on the Draft Personal Data Protection Proclamation of Ethiopia (Center for the Advancement of Rights and Democracy, August 2022) <https://www.cardeth.org/wp-content/uploads/2022/08/CARDs-Position-Paper-on-the-Draft-Personal-Data-Protection-of-Ethiopia-August-2022.pdf>accessed 26 January 2024.

[201] PDPP art 7/2.

[202] Ibid 7/2 (e).

required to fulfill functions of public authority, which inevitably involves the handling of personal data. However, even in such scenarios, the processing must align with the overarching mandate of protecting personal data.

In addressing sensitive personal data, the principle lays down specific provisions, such as requiring written consent specific to the processing purpose and ensuring that processing aligns with legal and non-commercial objectives of public organizations.[203] The legality principle is strictly adhered in the processing of the sensitive personal data requiring the processing to be necessary for medical treatment or legal proceedings, emphasizing the need for adequate protection at all times. The foundational principle is that the processing of such data is, by default, prohibited.

One of the key circumstances under which the processing of sensitive personal data is permitted is when the data subject has given explicit, written consent that is specific to the intended purpose of the processing. This consent acts as a cornerstone in the data protection framework, especially if the data is sensitive, to ensure that individuals retain control over how their sensitive information is used.

Another exception pertains to cases where the processing of sensitive data is necessary to safeguard the life and health of the data subject or another person, particularly when the data subject is unable to provide consent due to legal or physical impediments.

Transparency and fairness are another key element of the principle of legality that ensures that data subjects are fully apprised of how their personal data is handled. Transparency is crucial as it empowers individuals with the knowledge and understanding of the processing of their personal data, fostering a sense of trust and integrity in the process.[204] It also entails the obligation of the data controller or processor to communicate any relevant information about the data processing to the individual in a manner that is clear, straightforward, and accessible. Fairness implies that the processing should not be detrimental, unexpected, or misleading to the data subject.[205]

Moreover, this principle sets forth specific conditions to be met during the data processing. Firstly, the data controller or processor is required to implement suitable measures to provide information

[203] Ibid 7/2 (c).

[204] Ibid.

[205] Ibid art 12/1.

related to the processing in a concise and transparent format. Secondly, the processing should not be conducted in a way that adversely affects the data subject or in a manner that they would not reasonably anticipate. Finally, the processing must uphold the right of individuals to be informed and be executed in a manner that is clear, open, and honest.[206] This necessitates an ongoing responsibility for the data controller to consistently update data subjects. This includes verifying the processing of personal data related to the individual, providing a clear explanation of the processed data, disclosing all pertinent details regarding the data's source, and informing about the duration for which the data will be retained.[207]

#### 3.4.1.2. Principle of Purpose Limitation

The Principle of Purpose Limitation centers around the premise that personal data should only be collected for specific, explicit, and lawful purposes.[208] It mandates that the use of this data should align strictly with the initial objectives for which it was gathered. This principle is critical in preventing the misuse or repurposing of personal data for objectives incompatible with the original intent.[209] Additionally, any further processing or disclosure of personal data must align with the original purpose. An exception is made for processing related to archiving, research, or statistical purposes, provided that appropriate safeguards are in place to protect the data.[210]

For effective implementation, the purpose of data collection must be clearly communicated either directly to the data subject or through a notification to the relevant Authority.[211] This transparency ensures that both the data subject and regulatory bodies are aware of the intended use of the data.

Purpose limitation is frequently singled out as essentially important and fundamental principle in the field of data protection.[212] At the same time, the principle presents special challenges in practice where, ‘assessing the compatibility of any given operation with the purpose for which the data were originally collected is one of the most difficult and important tasks in supervising compliance

[206] Ibid art 12/1.

[207] Ibid art 25.

[208] Ibid art 13.

[209] Lee Bygrave (n 41) 91.

[210] PDPP art 13.

[211] Ibid.

[212] Ibid.

with data protection legislation, especially under current era of big data.[213] It addresses the challenge of maintaining data processing's predictability and relevance, aligning with data subjects' expectations and data controllers' intentions. This principle comprises three sub-principles: specificity and clarity in defining data collection purposes, the legality or legitimacy of these purposes, and the requirement that further data processing must not diverge from the original purposes.[214] The notion of 'legitimate' purposes extends beyond mere legality, incorporating broader ethical and social norms. The compatibility of secondary processing with initial purposes is also crucial, aiming not just for efficiency but for fairness and adherence to established data protection standards.

#### 3.4.1.3. Principle of Data Minimality

Complementing the Principle of Purpose Limitation is the Principle of Data Minimization. This principle underscores the necessity of collecting only data that is adequate, relevant, and not excessive in relation to its intended purpose.[215] The emphasis here is on restraint and relevance. By adhering to this principle, organizations limit their data collection to only what is necessary, minimizing the risk of unnecessary or invasive data accumulation. Another element pertaining data minimality is the issue of storage/retention of data. Storage limitation fundamentally restricts the duration for which personal data can be retained,[216] with a strong emphasis on the deletion of data once the initial purpose of collection has been achieved. According to this principle, personal data that has been processed for any specific purpose must not be kept beyond the necessary period required for that purpose.

However, if the retention of data is required or authorized by law or is reasonably necessary for a lawful purpose related to a function or activity, principle of minimality may be bypassed.[217] The principle also carves out a specific exemption for the retention of personal data records for

[213] Ibid.

[214] Ibid.

[215] Ibid art 6/1 (3).

[216] Ibid art 6/5.

[217] Ibid art 15/1

historical, statistical, or research purposes.[218] In these instances, there is a stipulation that adequate protections must be in place to safeguard these records from unauthorized access or use.[219]

Moreover, the law outlines obligations for individuals or entities who use personal data records to make decisions about the data subject. They are required to retain these records either for a period defined by law or a code of conduct, or, in the absence of such legal provisions, for a duration that allows the data subject ample opportunity to request access to their records.[220] This aspect of the principle ensures that individuals have the ability to review and understand how their personal data is being used, particularly in decision-making processes that directly affect them.

#### 3.4.1.4. Principle Proportionality and Necessity

The principle of proportionality stands as a cornerstone in the edifice of global legal doctrine, emerging as a pivotal organizing framework within the realm of jurisprudence. Predominantly in the European legal landscape, the proportionality test crystallizes as the paramount methodology for the juridical scrutiny of conflicts ensconced between fundamental rights and legitimate interests, prominently between the realms of privacy and security.[221] This principle is intrinsically aligned with the experiential fabric of human existence beyond the legal confines, necessitating merely a juxtaposition of two conflicting vectors. However, this requisite juxtaposition unveils the intricate nexus between the acts of balancing and the application of the proportionality principle, revealing how, in extremis, the latter may seamlessly transition into the former.[222] This nuanced understanding has led scholars to distinguish between 'weak' and 'strong' iterations of the proportionality test, where the former is seen as a mere equilibrium between privacy and security, inherently presupposing the mutual diminution of one in the enhancement of the other, and negating the potential for their concurrent existence.[223]

Within this paradigm Article 7/3 of the PDPP posits that data processing necessitated by public health crises, national emergencies, or the execution of public authority mandates, must align with

[218] Ibid art 53.

[219] Ibid arts 53 and 54.

[220] Ibid art 15/4.

[221] Olga Mironenko Enerstvedt (n 31) 179.

[222] Ibid.

[223] Ibid.

the proportionality principle, stipulating that limitations are permissible solely when they are indispensable and genuinely advance objectives of general interest.[224] This denotes that even when data processing objectives are deemed legitimate, their legitimacy is contingent upon the proportionality of the data collection and processing to the specified purpose, necessitating that such activities be necessary, adequate, relevant, and not excessive. Furthermore, if the predetermined objective can be attained without processing personal data or by processing a lesser volume of data,[225] then the processing may be deemed disproportionate and, consequently, illegitimate. However, the PDPP, despite establishing these prerequisites, falls short of providing explicit interpretations of what constitutes 'proportional,' 'necessary,' and related terms, thereby obscuring the objective assessment of proportionality.

These criteria can be categorized into several clusters, with the initial requirement being that the justification for the security measure's intrusion must be of sufficient significance to warrant the limitation of the right. This necessitates adherence to the principle of purpose limitation, as a clear understanding of the aim aids in determining further criteria for the measure's proportionality, such as the requisite data categories, processing types, data quality, etc. The paramount criterion for achieving the legitimate aim is the effectiveness of the measure, which must be demonstrably capable of fulfilling its specified purpose.[226] The second criterion, necessity, mandates that the measure is essential for achieving these objectives, with some scenarios demanding an even stricter standard of indispensability.[227] According to European Court Justice (ECJ) jurisprudence, a measure's proportionality is contingent upon the demonstration that less intrusive alternatives are non-viable.[228] In situations where multiple suitable measures are available, the least burdensome option should be prioritized.[229] Under the PDPP, the data controller and data processor are required to conduct data impact assessment an assessment of the necessity and proportionality of the

[224] PDPP arts 6/5 cum7/3.

[225] Ibid art 7/3/b.

[226] European Data Protection Board (n 202) para. 13.

[227] Ibid para 28.

[228] Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [2010] ECLI:EU:C:2010:662, paras 81, 86.

[229] Ibid.

processing operations in relation to the purposes.[230] This include that even in case of legitimate interests and public interests including the protection of national security, defense or public security and general public interest, including an economic or financial interest of the State if the processing of data is less necessary and disproportionate the data subject or the Authority may institute legal case in the court of law.[231]

#### 3.4.1.5. Principle of Data Accuracy

This principle emphasizes the necessity for data to not only be precise but also consistently updated to reflect current information. It is mandated that personal data must be kept accurate and up to date. The principle of accuracy comprises two key elements: firstly, it asserts that personal data should be accurate and, where necessary, regularly updated. This ensures that the data remains relevant and reliable over time.

The principle also acknowledges that there might be instances of inaccuracies.[232] In such cases, it is not considered a violation of the principle if the inaccuracy in the personal data accurately represents information received from the data subject or a third party.[233] This caveat applies under two conditions.

First, the data controller is obligated to have taken reasonable measures to verify the accuracy of the data, considering the purpose for which the data was originally obtained.[234] Thus, the responsibility lies with the data controller to ensure that the data is as accurate as possible, given its intended use.

Secondly, the data subject can also restrict the process of such personal data as provided under Article 14 and 30/1 (a) of the PDPP. Moreover, data subjects have the right to access their data and request corrections to any inaccuracies, thus indirectly maintaining oversight over their data.[235] If a data subject contends that the information is inaccurate and communicates this belief to the data controller, the recorded data should reflect this opinion. This is very important as it gives room for

[230] PDPP 47/3 (b).

[231] Ibid art 53.

[232] Ibid art 14.

[233] Ibid.

[234] Ibid art 14/1.

[235] Ibid art 27.

considering the perspective of the data subject in the accuracy of their personal data. Thus, it enhances the transparency, trust, and accountability expected in data handling practices.

#### 3.4.1.6. Principle of Data Security

Personal data should be processed in a manner that ensures the integrity, confidentiality, and security of the personal data.[236] The assessment of what constitutes an appropriate level of security must take into account the risks presented by data processing, particularly those stemming from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.[237] A failure to protect data security results in personal data breach. The definition of a breach is broad, covering incidents affecting the confidentiality, integrity, or availability of data. A data breach may involve confidentiality breach, unauthorized or accidental disclosure or access to personal data. It can also involve integrity breach related to unauthorized or accidental alteration of personal data.[238] Moreover, the third type of data breach can be availability breach i.e., accidental, or unauthorized loss of access to, or destruction of, personal data. A breach is considered a breach regardless of the resulting harm, whether accidental or deliberate. In this regard, the recent CBE incident is a good example.

In mid-March 2024, the Commercial Bank of Ethiopia (CBE) experienced a system glitch that allowed customers to withdraw or transfer more money than they had in their accounts.[239] Over 490,000 transactions with substantial amount of money resulted from this error, mostly from university students.[240]

In response, CBE issued an ultimatum for the customers to return the funds by visiting the nearest branch or using digital payment options.[241] When many did not comply, the bank escalated its

---

[236] Ibid art 6/6.

[237] Ibid art 17.

[238] Ibid.

[239] Borkena, 'Ethiopia's State Bank Gives Ultimatum to Clients Who Exploited System "Glitch" to Withdraw Money They Do Not Have' (Borkena, 21 March 2024) <https://borkena.com/2024/03/21/commercial-bank-of-ethiopia-state-bank-gives-ultimatum-to-clients-who-exploited-system-glitch-to-withdraw-money-they-do-not-have/#:~:text=Commercial%20Bank%20of%20Ethiopia%20(CBE)%20on%20Thursday%20announced%20an%20ultimatum,not%20have%20in%20their%20account> accessed 16 April 2024.

[240] Ibid.

[241] BBC News, 'Ethiopian bank gives deadline to return mistaken pay outs' (Addis Ababa, 20 March) <https://www.bbc.co.uk/programmes/p0hkq374> accessed 16 April 2024.

measures by releasing the names and images of the implicated customers.[242] CBE also warned that those who failed to return the money would face legal action and be held accountable due to the traceable nature of digital transactions.[243] The bank managed to recover about $10 million of the estimated $14 million withdrawn, although initial reports suggested losses could be as high as $40 million.[244]

Although the steps taken by CBE were intended to reduce major financial risks and recoup lost money, the public disclosure of personal data appears to conflict with the principles of data security and confidentiality outlined in Article 17 of the PDPP. The Bank's decision to publicize the images of the individuals may have been intended to mitigate significant financial losses, which is a serious risk. However, the action should be balanced against the harm that could result from unauthorized disclosure of personal data, particularly considering the sensitivity and potential consequences for the individuals involved. Thus, while the bank took steps to ensure the ongoing availability and integrity of its systems, the confidentiality of personal data was compromised by the public disclosure of customer identities.

This incident underscores the importance of robust measures to protect personal data and highlights the need for organizations to carefully balance security measures with privacy protections.

Data Security, therefore, requires implementing robust technical and organizational measures to safeguard personal data from unauthorized access, loss, damage, or unlawful processing.[245] This means that data controllers and processors are expected to adopt measures that not only prevent unauthorized access to data but also protect it from accidental loss or damage. This principle is not static; it evolves in tandem with technological advancements and takes into consideration the costs associated with implementing such security measures.

Furthermore, the principle of data security stipulates that these measures should align with the harm that could result from data breaches and the nature of the data that needs protection. This

---

[242] BBC News, 'Ethiopia's CBE Bank Recovers $10m Taken During Technical Glitch' (Addis Ababa, 26 March 2024) < https://www.bbc.com/news/world-africa-68663890> accessed 16 April 2024.

[243] Ibid.

[244] Ibid.

[245] Ibid art 17/1.

includes a comprehensive evaluation of various factors such as the state of the art in technology, the costs of implementation, the nature, scope, context, and purposes of data processing, as well as the potential risks to individuals' rights and freedoms.

Data security, among other things, can be achieved through the pseudonymization and encryption of personal data.[246] Additionally, it calls for regular testing, assessment, and evaluation of these security measures to ensure their effectiveness. This principle is primarily important when focusing on the confidentiality and integrity of personal data, especially in contexts where third-party data processors are involved.

The law mandates data controllers to take reasonable steps ensuring the reliability of their employees who have access to personal data in addition to ensuring the observance of the security measures in place.[247] This aspect of the principle emphasizes the importance of internal controls within an organization, recognizing that individuals within an entity can significantly impact data protection.

Furthermore, when a data controller employs a data processor, they must choose one that provides sufficient guarantees regarding the technical and organizational security measures of the data processing tasks.[248] This requirement underscores the need for a rigorous selection process for data processors, ensuring they have robust security measures. The principle also specifies that a data controller is not deemed compliant unless certain conditions are met. These include having a written contract with the data processor, ensuring the processor acts only on the controller's instructions, and requiring the processor to adhere to obligations equivalent to those imposed on the data controller. This obligation spans when a data transfer to a third-party jurisdiction is undertaken. According to Article 28 of the PDPP, the transfer of personal data to a third-party jurisdiction for processing is contingent on compliance with the Proclamation's provisions and subject to the third-party jurisdiction assurance of an appropriate level of protection for the data. Accordingly, factors to be considered for data transfer are the nature of the data, the intended

[246] Ibid art 17/4 (a).

[247] Ibid art 16/4.

[248] Ibid art 16/2.

processing operations' purpose and duration, the countries of origin and destination, and the legal and professional standards of data security in the third-party jurisdiction.[249]

The ECA plays a pivotal role in this framework. It is tasked with determining whether a third-party jurisdiction meets the required standard of data protection. In cases where a third-party jurisdiction lacks adequate protection levels, the ECA may authorize limited data transfers.[250] This authorization is subject to specific conditions, such as the data subject's consent and the Authority's discretion in severing or reducing certain data aspects. Accordingly, the conditions for cross-border transfer, include proof of adequate protection in the third-party jurisdiction, explicit consent of the data subject, necessity of the transfer, and transfers made from public registers.[251]

#### 3.4.1.7. Principle of Data Subject Influence

At the heart of data protection regulations lies a fundamental principle that individuals should possess the capability to engage with and exert a level of control over the processing of their personal data by third parties. This concept is called ‘data subject influence or Individual participation principle.’[252] However, the implementation of this principle extends beyond the apparent look of participation and encompasses a broader spectrum of rules designed to empower individuals in the context of data processing.

The principle of data subject influence is integrated into data protection laws through a series of rule categories. The first category includes rules aimed at raising public awareness about data processing activities. For instance, such rules may mandate data controllers to disclose essential information regarding their data processing activities to Data Protection Authorities, which in turn is required to be maintained in a publicly accessible registry.[253]

More crucial, perhaps, are the rules designed to inform individuals about the specifics of their own data being processed.[254] This set of rules can be further broken down into three main sub-categories: rules that mandate data controllers to collect data directly from the individuals in certain

[249] Ibid art 18.

[250] Ibid art 19/3.

[251] Ibid art 19.

[252] OECD, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (2002) 16.

[253] Olga Mironenko Enerstvedt (n 31) 168.

[254] PDPP art 24.

scenarios;[255] those mandating data controllers to inform data subjects about specific details of their data processing;[256] and those prohibit the processing of personal data without the explicit consent of the individual concerned.[257]

The overarching principle of individual influence over data processing encompasses a wide array of rules, many of which significantly overlap. The PDPP emphasizes duties of information dissemination and the orientation of individuals about their data processing, ensuring that this information is not only publicly available but also easily comprehensible. Individuals are to be informed about the nature of data being processed, the objectives of such processing, and the identity of the data collectors.[258] Furthermore, information regarding data protection measures, data sharing protocols, the identity of the responsible data officers, avenues for redress, and contact details for inquiries or concerns about data retention are also mandated to be provided.[259]

Individuals hold the right to object to data processing based on compelling legitimate grounds pertaining to their unique circumstances.[260] This right to object is intricately linked to the prohibition of certain data processing activities in the absence of the individual's consent. Consent, as defined within the framework of the PDPP, must be a freely given, specific, informed, and unequivocal indication of the individual's agreement to the processing of their personal data.[261]

However, ensuring that consent meets these criteria—being informed, specific, and freely given—poses significant challenges. The inherent power imbalance in data processing situations often renders consent a mere formality rather than a genuine expression of agreement.[262] Exceptions to the requirement for obtaining consent are notably broad, encompassing scenarios where data processing is deemed necessary for contract fulfillment, public interest tasks, or the protection of

[255] Ibid art 24/1.

[256] Ibid art 24/2.

[257] Ibid art 24/5.

[258] Ibid art 24.

[259] Ibid.

[260] Ibid art 29.

[261] Ibid art 8.

[262] Lee Bygrave (n 41) 170.

vital interests of the individual.[263] However, the law tried to tackle these challenges by stipulating the burden of proof to establish whether consent is given by the data subject in line with the requirements provided under the law on the data controller.[264]

Furthermore, individuals are entitled to access their data and request corrections to any inaccuracies, thereby indirectly exercising oversight over public security files to ensure their accuracy.[265] Noteworthy is the provision of rights for individuals to access data held about them by others, a right expansively defined under Article 25 of the PDPP to include not only direct data but also information regarding the processing methodologies, purposes, recipients, sources, and the logic behind automated data processing decisions.

The set of rules enabling individuals to object to data processing and demand rectification or erasure of their data in cases of inaccuracy, irrelevance, or illegal possession is closely tied to the consent-based prohibitions on data processing.[266] While the PDPP prominently features consent as a key precondition for data processing, it is often just one of several alternative prerequisites, which may dilute the practical reliance on consent in data processing activities.[267]

#### 3.4.1.8. Principle of Accountability

A more effective approach to safeguarding data involves the implementation of suitable legal frameworks, policy guidelines, and technological safeguards, centered around two main objectives: firstly, the regulated introduction of protective measures, and secondly, their responsible utilization. It's widely acknowledged that privacy protections are not necessarily achieved by discontinuing certain security initiatives but rather by subjecting them to stringent oversight, constraining the future exploitation of personal data, and guaranteeing their execution in a manner that is balanced and well-regulated.[268]

An accountability framework establishes a dynamic where one entity demands reporting from another and possesses the authority to enforce penalties. This can be differentiated into sanctioned

[263] PDPP art 7/2.

[264] Ibid art 8/5.

[265] Ibid art 27.

[266] Lee Bygrave (n 41) 170.

[267] Ibid.

[268] Daniel J Solove, 'Data Mining and the Security-Liberty Debate' (2008) University of Chicago Law Review 362.

accountability, characterized by a mutual recognition and acceptance of the obligations to report, and enforce, versus unilateral accountability, where one party assumes the right to hold the other accountable without an acknowledged mutual commitment. [269] Only the former can be deemed as genuine and robust accountability, capable of ensuring effective control mechanisms, such as the establishment of an independent evaluative body whose findings are binding for the operators of such measures. As argued by Etzioni, sufficiently robust accountability can render otherwise excessive powers permissible. While certain powers may remain unsuitable regardless of accountability measures, the preferred remedy for insufficient (or excessive) accountability is its recalibration rather than the outright rejection of the measure. [270] However, this raises the critical question of overseeing the overseers themselves. These insights hold true provided the system is fundamentally considered reliable, setting aside both governmental assurances of sufficient accountability and extreme civil libertarian objections that suggest an inherent mistrust in all authorities. Particularly challenging are issues of accountability towards external individuals impacted by the entity's actions. [271]

In the realm of data protection, there are emerging mechanisms aimed at addressing accountability between data subjects and data controllers. The PDPP mandates that data controllers bear responsibility and must demonstrate adherence to all principles of personal data handling, termed as 'accountability.'[272] To evidence such compliance, controllers are required to adopt suitable technical and organizational strategies, potentially including specific data protection policies.[273]

The PDPP outlines various duties and accountability responsibilities for data controllers, defined as individuals or entities with authority over data processing. This responsibility extends to data processors, who, though not employees of the controller, process data on their behalf.[274] These duties encompass a mandate for accountability, compelling controllers to ensure that all processing activities are in strict compliance with data protection principles and regulations. Moreover,

[269] Olga Mironenko Enerstvedt (n 31) 405.

[270] Amitai Etzioni, 'Implications of Select New Technologies for Individual Rights and Public Safety' (2002) Harvard Journal of Law and Technology 40.

[271] Olga Mironenko Enerstvedt (n 31) 405.

[272] PDPP art 52.

[273] Ibid arts 52 and 49.

[274] Ibid art 52.

controllers are obliged to register with the Authority, providing comprehensive details of their data processing operations.[275] Both controllers and processors must adhere to the PDPP's stipulations regarding any processing conducted by or for them, thereby reinforcing the principle of transparency. Data controllers are also expected to implement organizational measures such as robust data security protocols, maintaining a record of processing activities, conducting data protection impact assessments, and obtaining prior authorization or consultation from the Authority when necessary.[276] The appointment of Data Protection Officers is mandated for extensive processing of personal or sensitive data, with DPOs required to possess the necessary qualifications and tasked with ensuring compliance with the PDPP.[277]

The law obliges data controllers and, where applicable, data processors to incorporate data protection principles and safeguards into their processing activities right from the outset.[278] These entities must implement appropriate technical and organizational measures that effectively integrate personal data processing principles. This includes both at the planning stage and the actual processing phase. These measures should consider the state of the art, cost of implementation, nature, scope, context, and purposes of processing, as well as the potential risks to the rights and freedoms of individuals.[279] Furthermore, these measures must ensure that by default, only the personal data necessary for each specific processing purpose is handled.[280] This extends to the amount of data collected, the extent of its processing, storage duration, and accessibility.

### 3.4.2. Enforcement of Personal Data Protection Under the PDPP

The PDPP assigns crucial roles of enforcement to the Ministry of Innovation and Technology and the Ethiopian Communications Authority (herein after Authority). The Ministry is tasked with developing policies and strategies for personal data protection and overseeing their implementation,[281] while the Authority is charged with assessing compliance, issuing enforcement

[275] Ibid art 33.

[276] Ibid arts 46, 47, 48, and 49.

[277] Ibid art 40/4.

[278] Ibid art 49.

[279] Ibid art 49/2; European Data Protection Board, (n 202) para. 28.

[280] Ibid art 49/3; Ibid European Data Protection Board, para. 8.

[281] Ibid art 4.

orders, and conducting investigations into data breaches.[282] Managing grievances and deciding appeals against data controller decisions also fall under the Authority's responsibility.

However, the Authority's centralization of such substantial power has sparked discussions and worries, especially among media outlets and human rights organizations, raising critical questions about the balance between technological advancement and the protection of privacy rights.[283] One key issue is the inherent conflict of interest arising from the Authority's dual mandate to both promote telecommunications and information technology and enforce strict data protection norms. This may give rise to disputes, particularly when technological advancements require large-scale data usage.

Moreover, the Authority's expanded oversight of national communication systems introduces risks of compromising personal data protection in favor of broader national security or surveillance objectives.[284] Furthermore, the Authority's position is complicated by its accountability to the Prime Minister and the absence of an independent regulatory agency dedicated to data protection,[285] which could result in biases influenced by current political climates or governmental changes.

Globally, there is a trend towards establishing independent data protection mechanisms to ensure impartiality, minimize political influences, and enhance the fairness and transparency of data protection enforcement.[286] Critics have argued that such an independent body in Ethiopia could provide the necessary expertise and impartiality to oversee data protection efforts more effectively. Nonetheless, the government has decided to keep these duties under the Authority.[287]

---

[282] Ibid art 5.

[283] Ashenafi Endale, 'Critics Fear Comms Authority Personal Data Dominion, Impartiality in Legislative Wrangle' *The Reporter* (Addis Ababa, 13 January 2024) <https://www.thereporterethiopia.com/38279/> accessed 02 March 2024.

[284] Communication Service Proclamation No. 1148/2019, arts 6, 31, and 51.

[285] Ibid art 3/2.

[286] OECD, 'The OECD Privacy Framework' (2013) 29; Philip Schutz, 'Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective', Conference Paper in IFIP Advances in Information and Communication Technology (January 2012) 48.

[287] Ashenafi Endale (n 278).

The Authority's power extend to issuing detailed enforcement orders when data protection breaches are suspected, specifying necessary remedial actions and compliance timelines, and it retains the power to modify these orders if initial compliance seems unlikely.[288] It also plays a crucial role in investigating complaints, gathering necessary information on data processing activities, and, if required, restricting data controllers' operations to safeguard personal data.[289]

If a data subject is dissatisfied with a decision regarding their personal data, they can appeal to the Authority.[290] The Authority has the power to review decisions made by data controllers, and if necessary, can overturn these decisions.[291] Moreover, the Federal High Court has the jurisdiction to review the Authority's decisions. This judicial review can add another layer of oversight and ensure decisions comply with legal standards and principles of justice. However, the Higher Court's designation as an appellate court could narrow data subjects' judicial avenue thereby impacting their right to due process of law.

In cases where data processing does not meet lawful standards, the Authority can intervene.[292] However, the effectiveness of these mechanisms depends significantly on the Authority's ability to navigate its broad mandate without succumbing to conflicts of interest or political pressures. Thus, the Authority should establish a robust regulatory framework that uphold with the principles of the PDPP as well as human rights to effectively balance its mandate in technological/communication advancements and regulation of personal data protection.

[288] PDPP arts 55, 59, and 58.

[289] Ibid arts 48 and 54.

[290] Ibid art 61.

[291] Ibid.

[292] Ibid art 48.

## Chapter Four

# 4. Conclusion and Recommendation

## 4.1. Conclusion

The analysis of Ethiopia's personal data protection regime, specifically with regard to surveillance reveals a landscape in which the protection of privacy is often compromised by a convergence of broad legislative powers, the instrumental use of laws for political purposes, lack of sufficient procedural privacy safeguards, and the existence of inadequate oversight mechanisms that fail to regulate the extensive surveillance powers granted to the police and security service agencies.

The instrumentalization of laws to achieve political aims further exacerbates the vulnerability of individual rights under the guise of national security. This has contributed to unregulated data gathering, processing, storage, and access practices, jeopardizing human rights, most notably the right to privacy. Thus, it requires a critical reevaluation of the national security need justifications which is often used to justify surveillance to ensure the balance between country's security interests and individual freedoms are not disproportionate.

The lack of adequate legal limits on surveillance activities, coupled with weak judicial oversight mechanisms has contributed to a scenario where surveillance activities are at times arbitrary and not proportionate to their legal purposes. With all its drawbacks, the introduction of the Personal Data Protection law has addressed some of the challenges associated with personal data protection, such as unregulated data gathering, processing, and accessing by offering a comprehensive personal data protection framework that complies with international human rights standards.

However, despite the safeguards under the PDPP, addressing the challenge necessitates further synchronization of the existing legal frameworks with international human rights standards. The synchronization must also be comprehensive, extending beyond the legislative texts to actual practice to ensure that privacy and personal data protection are not only acknowledged but effectively protected.

Furthermore, the path to reform should involve multi-stakeholder engagement, utilizing the insights and expertise of various sectors including academia, civil societies, private sector, and government. Legislative amendments are also needed to ensure that Ethiopia's laws uphold the

principles in international human rights instruments. Additionally, an effective protection of privacy rights in the context requires strengthening the capacity of the justice system and raising the awareness of the populace, thus, special attention should be given to building the capacity of these groups.

### 4.2. Recommendations

To address the challenges in the personal data protection regime of Ethiopia in a manner that upholds the international human rights standards and best practices, the following key recommendations are proposed:

- Revise and tighten the legal frameworks surrounding surveillance including amending laws like the Computer Crime Proclamation No 958/2016 and Prevention and Suppression of Terrorism Crimes Proclamation No. 1176/2020 that grant broad surveillance powers to law enforcement and security agencies to ensure they contain clear, narrowly defined criteria that are necessary and proportionate to the intended security aims. The revision should introduce stringent judicial oversight mechanisms to prevent the misuse of surveillance powers. Furthermore, the amendments should introduce legal provisions that explicitly require the destruction of any data collected unlawfully or through rejected surveillance to further safeguard against arbitrary data processing and retention.
- Amend the PDPP provisions that gives power to the ECA to regulate personal data protection so that an independent neutral regulatory body to oversee the implementation of personal data protection can be established. This neutral body should be empowered to conduct audits to ensure compliance with privacy laws and the ethical use of surveillance technologies, handle complaints, and enforce penalties for non-compliance.
- The country should take measures to rebalance its national security measures with human rights. This involves setting higher thresholds for surveillance under national security pretexts and ensuring such measures are subject to rigorous judicial oversight.
- Initiatives to strengthen the capacity of law enforcement and the judicial system on personal data protection and privacy rights should be prioritized. Thus, the government and other partners should design training programs and allocate resources to build the competencies of these institutions. Programs to enhance the public's awareness of privacy

rights should also be given due attention, these initiatives should fit Ethiopia's cultural context to promote a balanced understanding of individual rights versus communal values.

- The government and the private sector should invest in robust technological infrastructures to safeguard personal data against breaches and unauthorized access as well as surveillance.
- The government should encourage organizational self-regulation through best practices like privacy by design and regular privacy impact assessments as indicated under the PDPP.
- The government should introduce a regular reporting mechanism on the use of surveillance technologies and the outcomes of surveillance activities to make it accountable to the public. These reports should be made public and details like justifications for surveillance operations, their effectiveness, and any issues or abuses identified should be covered in the reports.
- The government, private sector, academia, civil society organizations, and rights bodies should work closely with each other as well as the international human rights mechanisms to ensure the adherence of the national personal data protection practices with global human rights standards. This includes adopting recommendations from human rights bodies like the Human Rights Committee.

# Bibliography


**Cases**

- Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [2010] ECLI:EU:C:2010:662, paras 81, 86.
- Kidane v Government of Ethiopia [2016] USCA DC 16-7081 (Court of Appeals, DC Circuit). https://www.cadc.uscourts.gov/internet/opinions.nsf/E0C614D73F037CAD852580E3004EE648/$file/16-7081-1665840.pdf.

**Legislations**

- African Charter on Human and Peoples' Rights.
- Charter of Fundamental Rights of the European Union (2009).
- Civil Code of the Empire of Ethiopia 1960.
- Communication Service Proclamation No. 1148/2019.
- Constitution of the Federal Democratic Republic of Ethiopia (1995).
- Electronic Signature Proclamation No. 1072/2018.
- European Convention on Human Rights.
- Federal Income Tax Proclamation No. 979/2016.
- Financial Consumer Protection Directive No. FCP/01/2020.
- Freedom of Mass Media and Access to Information Proclamation No. 590/2008.
- Information Network Security Agency Re-establishment Proclamation No. 808/2013.
- International Covenant on Civil and Political Rights.
- Personal Data Protection Proclamation No. 1321 2024.
- Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No 780/2013.

- Prevention and Suppression of Terrorism Crimes Proclamation No. 1176/2020.
- Revised Constitution of Ethiopia, 1955.
- Telecom Fraud Offense Proclamation No. 780/2013.
- Telecom Fraud Proclamation No.761/2012.
- Universal Declaration of Human Rights.


**Secondary Sources**


- Abebe Sintayehu & Fiseha Eyerus, 'Ethiopia is Moving Towards Data Protection', Renew Capital, 8 Jan 2022 https://www.renewcapital.com/newsroom/ethiopia-is-moving-towards-data-protection.
- Almeida Denise, Shmarko Konstantin, and Lomas Elizabeth, 'The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks' (2022) 2 AI and Ethics.
- Benchlouch Ariela & Sher Gai, 'The privacy paradox with AI' (October 2023) Reuters https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/.
- Brechenmacher Saskia, 'Surveillance and State Control in Ethiopia' (2017) Carnegie Endowment for International Peace.
- Bygrave Lee A, 'The Place of Privacy in Data Protection Law' (2000) 24(1) UNSW Law Journal.
- Cohen Julie E, 'What is Privacy For?' (May 2013) 126(7) Harvard Law Review 1910.
- Cooper Kate, 'Closely Watched Households: Visibility, Exposure, and Private Power in the Roman "Domus"' (2007) Oxford University Press 5.
- DeCew Judith Wagner, 'The Scope of Privacy in Law and Ethics' (August, 1986) 5(2) Law and Philosophy.

- Etzioni Amitai, 'A Communitarian Perspective on Privacy' (2000) 32 Connecticut Law Review.
- Flynn Susan & Mackay Antonia, 'Surveillance and Spatial Performativity in the Scenography of Tower Lucy Thornett in' (2019) Palgrave Macmillan.
- Fried Charles, 'Privacy' in: Philosophical Dimensions of Privacy, edited by F. D. Schoeman (1984) Cambridge University Press.
- Glancy Dorothy J, 'The Invention of the Right to Privacy' (1979) 21 Arizona Law Review.
- Grinberg Daniel, Chilling Developments: Digital Access, Surveillance, and the Authoritarian Dilemma in Ethiopia, Surveillance and Society, 2017.
- Himma Kenneth Einar, 'Privacy Versus Security: Why Privacy is Not an Absolute Value or Right' (2007) 44 San Diego Law Review 904.
- Human Rights Council, 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development' (51st sess, agenda items 2 and 3, UN Doc A/HRC/51/42, 2022) https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf?token=TOPkuzNqYUJ2ydFKGw&fe=.
- Human Rights Watch, 'They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia' (March 2014) https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia.
- 38. Kasper Debbie V S, 'The Evolution (Or Devolution) of Privacy' (2005) 20(1) Sociological Forum.
- Lessig Lawrence, 'Privacy as Property' (Spring 2002) 69(1) Social Research.
- Locke John, 'Two Treatises of Government' (1860) McMaster University Archive of the History of Economic Thought.

- Lum Kristian, 'Predictive Policing Reinforces Police Bias' (October, 2016) Human Rights Data Analysis Group https://hrdag.org/2016/10/10/predictive-policing-reinforces-police-bias/.
- Lynskey Orla, 'The Foundations of EU Data Protection Law' (2015) Oxford University Press.
- MacKinnon Catharine A, 'Feminism, Marxism, Method, and the State: Toward Feminist Jurisprudence' (1983) University of Chicago Press 635.
- McCloskey H. J., 'Privacy and the Right to Privacy' (1980) 55 Philosophy.
- OECD, 'Mapping Approaches to Data and Data Flows' (2020) Report for the G20 Digital Taskforce, OECD Publishing.
- OECD, 'The OECD Privacy Framework' (2013) 29. See also Schutz Philip, 'Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective', Conference Paper in IFIP Advances in Information and Communication Technology (January 2012).
- Power Daniel J., Heavin Ciara, O'Connor Yvonne, 'Balancing privacy rights and surveillance analytics: a decision process guide' (2021) 4(2) Journal of Business Analytics.
- Roth Louise Marie, 'The Right to Privacy Is Political: Power, the Boundary between Public and Private, and Sexual Harassment' (1999) 24(1) Law & Social Inquiry 50.
- Sekulovski Jordanco, 'The Panopticon Factor: Privacy and Surveillance in the Digital Age'.
- Sher Gai & Benchlouch Ariela, 'The privacy paradox with AI' (October 2023) Reuters https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/.
- Solove Daniel J, 'Data Mining and the Security-Liberty Debate' (2008) University of Chicago Law Review.

- Solove Daniel J., 'Understanding Privacy' (May 2008) GWU Legal Studies Research Paper No. 420, available at SSRN: https://ssrn.com/abstract=1127888.
- Stach Christoph, 'Data Is the New Oil–Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration' (2023) 15 Future Internet.
- Steves Valerie, 'Now You See Me: Privacy, technology and Autonomy in the Digital Age' (2023) University of Ottawa.
- UN General Assembly, 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development', Human Rights Council Seventeenth session, Agenda item 3, A/HRC/17/27 (2011).
- UNCTAD, 'Ethiopia's drive to advance digital transformation' UNCTAD/BRI PROJECT/PB 02 (April 2022).
- Véliz Carissa, 'Democracy, Politics, Privacy and Surveillance' (6 April 2021) https://www.bostonreview.net/articles/why-democracy-needs-privacy/.
- Wacks Raymond, 'Privacy: a very short introduction' (2010) Oxford University Press.
- Warren Samuel D. & Brandeis Louis D., 'The Right to Privacy' (1890) 4(5) Harvard Law Review.
- Westin Alan F., 'Privacy and Freedom' (1968) 25(1) Washington and Lee Law Review 170.
- Yilma Kinfe Michael, 'Data privacy law and practice in Ethiopia' (2015) International Data Privacy Law 7; Himma Kenneth Einar, 'Privacy Versus Security: Why Privacy is Not an Absolute Value or Right' (2007) 44 San Diego Law Review 904.
- Zuboff Shoshana, 'The Age of Surveillance Capitalism: the Fight for a human future at the new frontier of power' (2020) Harvard University Press.
- 'The Reporter', 'Critics Fear Comms Authority Personal Data Dominion, Impartiality in Legislative Wrangle' (13 January 2024) https://www.thereporterethiopia.com/38279/.