ECSU
Est. 1995
BUILDING CAPACITIES IN THE PUBLIC SERVICE

# Ethiopian Journal of Legal Studies

ISSN: 2789-2379

## Articles

• "The African Criminal Court": A Regional Adjunct to or Competing Court with the ICC?

• Global-Regulation of Cyberspace Security and the Ethiopian Context

• Exploring Safeguards of Privacy Right in the Digital Age: How to Regulate Invisible Intrusion in Ethiopia?

• The Requirement of Leave without Pay to Run for Election in Ethiopia: A Subtle Deprivation of Civil Servants or Levelling a Playground in Quest for Fairness?

## Reflections

• The Notion of 'Business': An activity? A responsibility? An entity? Or A property? (Issues for Consideration)

## Case Comments

• የፍቺ ውሳኔ የጋብቻ ውልን ቀሪ ያደርጋል ወይስ አያደርግም?

Volume 1 Number 2 Dec, 2021

# Ethiopian Journal of Legal Studies

ISSN: 2789-2379

## Articles


- "The African Criminal Court": A Regional Adjunct to or Competing Court with the ICC?
- Global-Regulation of Cyberspace Security and the Ethiopian Context
- Exploring Safeguards of Privacy Right in the Digital Age: How to Regulate Invisible Intrusion in Ethiopia?
- The Requirement of Leave without Pay to Run for Election in Ethiopia: A Subtle Deprivation of Civil Servants or Levelling a Playground in Quest for Fairness?


## Reflections


- The Notion of 'Business': An activity? A responsibility? An entity? Or A property? (Issues for Consideration)


## Case Comments


- የፍቺ ውሳኔ የጋብቻ ውልን ቀሪ ያደርጋል ወይስ አያደርግም?

# Correspondence

**The Ethiopian Journal of Legal Studies (EJoLS) invites submission of scholarly articles, case comments, reflections, book review and other academic works for publication. Submission can be sent to the Managing Editor of the Journal in the following addresses:**

**Email:ejols.ecsu@gmail.com or lnanebo@gmail.com**

**P.O.Box: Managing Editor EJoLS,**

**School of Law and Federalism,**

**Ethiopian Civil Service University,**

**P. O. Box 5648,**

**Addis Ababa, Ethiopia**

The Ethiopian Journal of Legal Studies is published twice a year by the School of Law and Federalism, Ethiopian Civil Service University. Editorial and general offices are located in the Diplomacy Building next to room No. 018.

The Journal invites the submission of unsolicited articles, essays, and book reviews, comments, reflections, and case comments. Article submission should include an abstract of not more than 250 words.



**Disclaimer: The opinions expressed in the Journal are those of the authors, and do not necessarily reflect those of the School of Law and Federalism, the editors, the editorial board, or the University.**

# Ethiopian Journal of Legal Studies

# EJoLS

## Advisory Board Members

| | |
|---|---|
| Professor Fikre Desalegn | President of ECSU |
| Dr. Alemayehu Debebe | V/President for Research and Community Service at the ECSU |
| Professor Dolores A. Donovan | University of San Francisco |
| Professor Faizan Mustafa | Vice Chancellor of |
| Professor Christian Okeke | Director or Center for International Legal Studies, Golden Gate University, San Francisco |
| Professor Awobeami Ojebode | University of Ibadan, Nigeria |

## Editorial Board Members

| | |
|---|---|
| Lantera Nadew Anebo (LL.B, LL.M. SJD) | Editor-in-Chief, Assistant Prof., ECSU |
| Mussie Mezgebo, (LL.B.,LL.M.) | Managing Editor, Assistant Prof., ECSU |
| Assefa Fisseha (LL.B, LL.M. PhD) | Prof., AAU |
| Getachaw Assefa (LL.B, LL.M. PhD) | Associate Prof., AAU |
| Marshet Tadesse (LL.B. LL.M. PhD) | Assistant Prof., ECSU |
| Dejene Girma (LL.B., LL.M. PhD) | Assistant Prof., ECSU |
| Muradu Abdo (LL.B. LL.M. PhD) | Associate Prof., AAU |

### Language Editor

| | |
|---|---|
| Waqgari Negari (BA, MA, PhD) | V/President for Training and Consultancy Service |

# Full Time Academic Staff of the School of Law and Federalism

| Name | Academic Qualification and Rank |
|---|---|
| Mussie Mezgebo | LL.B., LL.M., Assistant Professor, Head, School of Law and Federalism, |
| Tesfaye Abate | LL.B., LL.M, LL.D, Assistant Professor, Dean College of Leadership and Governance, |
| Bisrat Tekleu | LL.B. LL.M, Lecturer, |
| Dejene Girma | LL.B, LL.M, PhD, Assistant Professor, |
| Eyerusalem Jima | LL.B. LL.M, Lecturer, |
| Fasil Alemayehu | LL.B, LL.M, Assistant professor, |
| Gedion Mezmur | BA, MA, PhD Candidate, Lecturer, |
| Gosaye Birhanu | LL.B, LL.M, Lecturer, |
| Habtamu Hailemeskel | LL.B. LL.M, Lecturer, |
| Lantera Nadew | LL.B, LL.M, LL.M, SJD Assistant Professor, |
| Marshet Tadesse | LL.B, LL.M PhD ,Assistant Professor, |
| Misganaw Kifele | LL.B. LL.M, PhD, Assistant Professor, |
| Mohahmmed Abdo | LL.B, LL.M, PhD, Assistant Professor, |
| Teguadda Alebachew | LL.B., LL.M, Assistant Professor, |
| Tihtina Getaneh | LL.B., LL.M. PhD, Assistant Professor, |
| Tsega Andualem | LL.B., LL.M, SJD, Assistant Professor, |
| Woldemichael Missebo | LL.B., LL.M, PhD Candidate, Lecturer, |
| Girum Kenfemichael | BA, MA, PhD Assistant Professor, |
| Yemserach Legesse | LL.B, MA, Lecturer, |
| Zerhun Geleta | LL.B, MA, PhD Assistant Professor. |

# Editorial Note

The Ethiopian Journal of Legal Studies (EJoLS) has a motto of advancing the Ethiopian legal literature a step ahead. EJoLS is a double-blind peer reviewed biannual journal that publishes articles of high standard triggering toward tackling national, regional or international socio-legal issues.

Due to rigorous publication requirements several submissions were either disregarded or sent back to authors for possible modification in accordance with the acceptability guidelines of the EJoLS. The Editorial Board of the Journal finally selected four best articles that would contribute to the Ethiopian legal literature and offer policy options. Further a reflection that would settle several issues involving the notion of business and an instructive case comment to be published in this issue are included.

The first article examines the Malabo Protocol that apparently extends the scope African Court of Justice and Human Rights. The Protocol was included in the international criminal section of the Human Rights and General Affairs Section of the Court. This necessarily ensues jurisdictional issues, whether the Protocol simply expands the scope of Court or whether it is a supportive law of International Criminal Court. Other related issues, rules, concepts and doctrines are briefly discussed. The second article explores national and global cyber security regulation. Cybercrime is the issue of global community. Invisible cyberspace violators can knock all doors and destroy or steal asset or commit undefendable crimes. Cyber security issue has been threatening Ethiopia. Ethiopia's alleged historical enemies not only indirectly involved in the ongoing war, but also attempting to disrupt vital infrastructure through invisible actors violating Ethiopia's cyberspace. As we have law of war cybercrime or cyber war should be regulated and controlled. The article endeavors to shed light on the battle for regulation of cyberspace. The third article deals with privacy issues. Everybody aspires certain acts or actions to be kept private. There are boundaries to know about one's identify, body, relationship and so forth. But in the digital age, it has been hard to protect privacy in the traditional way. Today, surveillance cameras are planted in all corners of city, government offices, private businesses, in transportation services and so forth. However, individuals' interest for privacy and security interest should be well balanced. The article examines how privacy and security interest may be

regulated. The fourth articles assess Ethiopian election law vis-à-vis the right of civil servants to run for elected public offices. The article examines how the current election law subtly denies Ethiopian civil servants to be elected. It argues, given the poor economic status of Ethiopian civil servants, the requirement to take leave without pay restrains civil servants from running for elected offices. The article assesses international and nation law, experiences of other jurisdiction and suggested for modification of the current Ethiopian election law.

I would like to express my appreciation to the contributors, editorial board members, the School of Law and Federalism, ECSU, the College of Leadership and Governance, and the AVP, for Research and Consultancy, the University for the Unwavering Support and encouragement for realization of this Journal.

The Editor – in – Chief

# Contents Page

## Articles (Peer Reviewed)


- "The African Criminal Court": A Regional Adjunct to or Competing Court with the ICC? 1

  *Dr. Marshet Tadesse, Eyerusalem Jima, and Henok Wolka*

- Global-Regulation of Cyberspace Security and the Ethiopian Context 29

  ***F**ikreselassie Getachew*

- Exploring Safeguards of Privacy Right in the Digital Age: How to Regulate Invisible Intrusion in Ethiopia? 61

  *Yisak Abraham*

- The Requirement of Leave without Pay to Run for Election in Ethiopia: A Subtle Deprivation of Civil Servants or Levelling a Playground in Quest for Fairness? 89

  *Nesredin Ahmed*


## Reflections


- The Notion of 'Business': An activity? A responsibility? An entity? Or A property? (Issues for Consideration) 115

  *Dr. Lantera Nadew*


## Case Comments


- የፍቺ ውሳኔ የጋብቻ ውልን ቀሪ ያደርጋል ወይስ አያደርግም? 126

  በዶ/ር ደጀኔ ግርማ ጃንካ

# "The African Criminal Court": A Regional Adjunct to or Competing Court with the ICC?

Marshet Tadesse *
Eyerusalem Jima **
Henok Wolka ***

**Abstract**

*In 2014, African Union adopted the Malabo Protocol that expanded the jurisdiction of the African Court of Justice and Human Rights. The Protocol added an international criminal law section, which has subject-matter jurisdiction over 14 crimes, to the existing Human Rights and General Affairs Sections of the African Court. The International Criminal Law Section has overlapping subject matter jurisdiction with the International Criminal Court as regards the four core crimes namely genocide, war crimes, crimes against humanity, and aggression. The complementary principle of the Rome Statute explicitly regulates the relationship between the national criminal jurisdictions and the ICC. It does not however mention, let alone regulate, the Court's symbiosis with regional criminal courts like the International Criminal Law Section of the African Court. The Statute of the African Court does not even mention the ICC, much less regulate the latter's relationship with the African Court. The absence of a clear provision that addresses the relationship between the ICC and regional criminal courts raises many questions. This begs the question of whether the International Criminal Law Section is created as a regional adjunct to the ICC or designed to compete with the ICC. This article examines the possible relationship that should exist between the International Criminal Law Section of the African Court and the ICC, if and when, the former becomes operational. The article, by advancing a teleological interpretation of the applicable laws of the courts, concludes that the spirit of the complementarity principle of the ICC accommodates not only the establishment of regional arrangements like the International Criminal Law Section of the African Court but also their primacy jurisdiction over the ICC.*

**Keywords:** African Criminal Court, International Criminal Law, African Union, International Criminal Court, Malabo Protocol, Statute of African Court, Complementarity

## 1. Setting the Context: A Prelude

The African Court has gone through several developments before taking its present shape with the International Criminal Law Section as one of its three sections. The first court introduced by the Organization of African Unity (OAU) is the African Court on Human and Peoples Rights (ACHPR), which is based in Arusha. This court was established in 1998 by the Protocol to the African Charter on Human and People's Rights.[1] The Court complements the protective mandate

* LL.B., LL.M. PhD, Assistant Professor, School of Law and Federalism, ECSU.
**LL.B., LL.M., Lecturer, School of Law and Federalism, ECSU.
*** LL.B., LL.M., Human Rights Officer, Monitoring and Investigation, EHRC.

of the African Commission on Human and Peoples` Rights.[2] The Court has jurisdiction over all cases and disputes submitted to it concerning the interpretation of the protocol and other human rights instruments ratified by the states.[3] African Commission on Human and People's Rights, the state parties, and the African Intergovernmental Organizations have the right to file an application to the Court.[4] Individuals and non-governmental organizations (NGOs) are also allowed to submit cases directly to ACHPR if a state makes a declaration under Article 34(6) of the Court's Protocol which allows individuals and NGOs to directly access the court.[5] The Court also at the request of member states of the African Union (AU), any of its organs, or any African organization recognized by the AU, provides an advisory opinion on any legal matter relating to the African Charter or any other relevant human rights instruments.[6]

The other court under the auspices of the AU is the African Court of Justice (ACJ), which was established by the AU Constitutive Act.[7] However, its composition and functions were left to be finalized in a separate protocol at a later time,[8] which was adopted in July 2003.[9] The ACJ has jurisdiction over general affairs such as interstate disputes, [10] interpretation and applications of matters arising from the application or implementation of the African Union Constitutive Act.[11]

---

.

1 Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, (opened for signature 10 June 1998, entered into force 25 January 2004) (ACHPR Protocol).

2 *Id*, Art. 2.

3 *Id*, Art. 3.

4 *Id*, Art. 5(1).

5 *Id*, Art. 5(3). Thus far ten countries namely Burkina Faso, Malawi, Mali, Tanzania, Ghana, Rwanda, Coted'Ivoire, Benin, Tunisia, and the Gambia) have made the declaration under article 34(6) accepting the competency of the court to receive cases from NGO's and individuals. At the time of writing four countries Tanzania, Rwanda, Coted'Ivoire, and Benin have withdrawn their declaration. Available athttps://www.african-court.org/wpafc/declarations/last visited September 2021.

6 *Id,* Art. 4(1). For more discussion on ACHPR Protocol see Tom Gerald Daly and Micha Wiebusch, "The African Court on Human and Peoples' Rights: Mapping Resistance against a Young Court," *International Journal of Law in Context*, Vol. 14 Issue, 2 (2018). See also "Practical Guide The African Court on Human and Peoples' Rights towards the African Court of Justice and Human Rights, "*International Federation for Human Rights*," (2010). Available at https://www.fidh.org/IMG/pdf/african_court_guide.pdf last visited September 2021.

7 Organization of African Unity, Constitutive Act of the African Union, (opened for signature 1 July 2000 entered into force 26 May 2001) (Constitutive Act of the African Union) Arts. 5(1)(d) and 18(1).

8 *Id,* Art. 18 (2).

9 Protocol of the Court of Justice of the African Union, (opened for signature 11 July 2003 entered into force 11 February 2009) (ACJ Protocol).

10 Ademola Abass, "The Proposed International Criminal Jurisdiction for the African Court: Some Problematical Aspects," *Netherlands International Law Review,* Vol. 60, (2013), pp. 30-31.

11 Art. 19(1) and (2) of the ACJ Protocol.

Although the Protocol establishing the ACJ has entered into force,[12] the Court has not been operationalized to date.[13]The discussion over the merger of the ACHPR with the ACJ by the AU Assembly of Heads of State and Government which began in 2004 is raised as a justification for not operationalizing the ACJ.[14]

The AU Assembly decided in 2004 that the ACJ should be merged with the ACHPR.[15] In 2008 the AU adopted a Protocol that merged the two Courts (ACHPR with ACJ) and created the African Court of Justice and Human Rights (ACJHR).[16] The main reason for the amalgamation of the two Courts was premised on the need to utilize the limited resources available in an efficient way.[17] The merged court is composed of two sections: the General Affairs Section and the Human Rights Section.[18] The General Affairs Section is empowered to hear all cases other than those bestowed to the Human Rights Section.[19] On the other hand, the Human Rights Section is mandated to hear all cases concerning human rights or matters that fall under the jurisdiction of the ACHPR.[20] At the time of writing 33 African States have signed the Merger Protocol and only eight (8) countries have ratified it.[21] Thus, the Merger Protocol has not yet entered into force as the minimum 15 ratifications required for it to enter into force are far from met.[22]

---

12 At the time of writing 45 Countries have signed and 19 countries have ratified the ACJ Protocol. Status List available at https://au.int/en/treaties/protocol-court-justice-african-union last visited September 2021.

13 Abass, *supra* note 10, p. 31.

14 *Id*.

15 African Union Decision on the Seats of the African Union, Assembly of the African Union, Third Ordinary Session, 6–8 July 2004 Assembly/AU/Dec.45 (III) Rev.1 , para. 4 (Decision on the seat of the AU); See also African Union, Decision on the Merger of the African Court on Human and Peoples' Rights and the Court of Justice of the African Union, EX.CL/Dec.165 (VI), Executive Council, Sixth Ordinary Session, 24–28 January 2005.

16 Protocol on the Statute of the African Court of Justice and Human and Human Rights, (adopted 1 July 2008), Assembly /AU/Dec.196 (XI) (hereinafter Merger Protocol).

17 Vincent O. Nmehielle, "Saddling the new African Regional Human Rights Court with International Criminal Jurisdiction: Innovative, Obstructive, Expedient?," *African Journal of Legal Studies,* Vol. 7, (2014), p. 9; Olufemi Elias, "Introductory Note to the Protocol on the Statute of the African Court of Justice and Human Rights," *International Legal Materials,* Vol. 48, (2009), p. 334; See also Matiangai Sirleaf, "The African Justice Cascade and the Malabo Protocol," *International Journal of Transitional Justice* Vol. 11, (2017), pp. 29 and 71.

18 Art. 16 of the Merger Protocol.

19 *Id*, Art. 17(1).

20 *Id*, Art. 17(2).

21 Angola, Benin, Burkina Faso, Comoros, Liberia, Gambia, Libya, and Mali have ratified the Protocol. See Status List available at https://au.int/en/treaties/protocol-statute-african-court-justice-and-human-rights last visited September 2021.

22 Art. 9(1) of the Merger Protocol.

Although the AU has made various improvements to the African Court structure, it is not complacent with all the previous revisions. In June 2014, the AU Heads of State and Government held its ordinary meeting in Malabo, Equatorial Guinea and adopted the Malabo Protocol; which in its annex included the Statute of the African Court of Justice and Human and Peoples' Rights as the applicable law of the court.[23] The Malabo Protocol expands the jurisdiction of the African Court of Justice and Human and Peoples' Rights (hereafter 'the African Court')[24] and vests this court with jurisdiction over international and transnational crimes.[25] The Malabo Protocol has not yet entered into force as there is no single ratification, let alone the required 15 ratifications for it to enter into force.[26] The Malabo Protocol established a tripartite court structure by amalgamating three distinct courts into a single judicial institution. Thus, the African Court has three sections, namely the General Affairs Section, the Human and Peoples' Right Section and the International Criminal Law Section, ('the African Criminal Court' or 'the ACC').

---

[23] Protocol on Amendments to the Protocol on the Statute of the African Court of Justice and Human Rights opened for signature 27 June 2014 (hereafter referred to as the 'Malabo Protocol'); and the Statute of the African Court of Justice and Human and Peoples' Rights, an annex to the Malabo Protocol.

[24] In Malabo Protocol, the name of the tripartite court structure is referred to as African Court of Justice and Human and Peoples' Rights'. See Arts. 1 and 8 of the Malabo Protocol; Art. 2 of the African Court Statute. Although inclusion of "Peoples" which was omitted in the Merger Protocol is apt for it recognizes the unique third generation rights in the African Charter on Humans and Peoples' Rights, the nomenclature of the Court is problematic. Hence criticized, rightly so, for obviating the international criminal jurisdiction of the Court. Marshet, for instance argued that this name might be appropriate to express the nature of the two-section court created by the Merger Protocol. However, the addition of the third section makes this name inappropriate and suggests that the title of the court should be simply the " African Court" as using the "African Court of Justice Human and Peoples' Rights and International Criminal Law Section would make the nomenclature unnecessarily long. See Marshet Tadesse Tessema "African Regional Developments-Challenges or Chance for the International Criminal Court? Three Courts in One: The African Criminal Court" in Gerhard Werle and Andreas Zimmermann (eds) *The International Criminal Court in Turbulent Times* (Vol. 23, 2019 TMC Asser Press), p. 45. See also Abass, *supra* note 10, p. 32; Viljoen, on the other hand, suggests having two separate courts. As the establishment of an African Court with international crimes jurisdiction has the potential of being a stumbling block to the existing human rights protection he suggests the establishment of separate judicial body, distinct from the two sections that are anticipated under the Merger Protocol for international crimes jurisdiction. See Frans Viljoen, "AU Assembly should consider human rights implications before adopting the Amended Merged African Court Protocol," AfricLaw, (2012). Available athttps://africlaw.com/2012/05/23/au-assembly-should-consider-human-rights-implications-before-adopting-the-amending-merged-african-court-protocol/ last visited September 2021.

[25] Art. 3 of the Malabo Protocol; Art.16 of the African Court Statute.

[26] The countries that have signed the Protocol are Benin, Chad, Comoros, Congo, Equatorial Guinea, Ghana, Guinea-Bissau, Guinea, Kenya, Mauritania, Sierra Leone, Togo, Mozambique, Sao Tome and Principe and Uganda, but no African country has ratified the Protocol, see Status list available at https://au.int/en/treaties/protocol-amendments-protocol-statute-african-court-justice-and-human-rightslast visited September 2021.

Following the adoption of the Malabo Protocol that established the ACC, scholars raised different and diverging views on the plausible relationship between the ACC and the ICC. The Rome Statute of the ICC does mention, let alone address its relationship with regional criminal courts (RCCs) like the ACC. Consequently, some writers even questioned the legality of establishing RCCs, in this case, the ACC,[27] others raised concerns regarding the possible problem that will pop up due to jurisdictional overlaps between RCCs and the ICC.[28] On the other hand, as 33 African states still commit to the ICC as states parties, the introduction of a new regional court having criminal jurisdiction over the same crimes will result in double or probably competing obligations.[29]

The Statute of the African Court/ ACC does not also mention, much less address its relationship with the ICC, albeit there is clear jurisdiction overlaps as far as the core crimes and the 33 African countries which are parties to the Rome Statute. Simply put, the ACC has subject matter jurisdiction over the same four core crimes as the ICC;[30] and ten additional transnational crimes.[31]

Thus, the issue of whether the ACC is created as a regional adjunct to the ICC or as a competing court or vice-versa is research worthy. Therefore, this article by employing doctrinal research methodology and through teleological analysis of the relevant provisions of the Rome Statute

---

27 Chacha Bhoke Murungu, "Towards a Criminal Chamber in the African Court of Justice and Human Rights," *Journal of International Criminal Justice*, Vol. 9, (2011), p. 1067. Murungu questioned the doctrinal compatibility of creation of regional criminal courts with Rome Statute of the ICC.

28 Abass, *supra* note 10, p. 27.

29 Erika De Wet "Concurrent Jurisdiction of the International Criminal Court and the African Criminal Chamber in the Case of Concurrent Referrals" in Charles C Jalloh, Kamari M Clarke and Vincent O Nmehielle (eds) *The African Court of Justice and Human and Peoples' Rights in Context: Development and Challenges* (1st edn, 2019, Cambridge University Press), p. 186; Tefera Degu Addis, "Some Reflections on the Current Africa's Project on the Establishment of African Court of Justice and Human Right (ACJHR)," (*AfricLaw*, 29 June 2015).Available at Some reflections on the current Africa's project on the establishment of African Court of Justice and Human Right (ACJHR) | AfricLaw last visited September 2021.

30 Cf. Art. 28A of the African Court Statute with Art.5 of the Rome Statute.

31 See Art. 28A of the African Court Statute. Abass, argues that not all offences that belong to the subject-matter jurisdiction of the prospective African Court would qualify as serious international crimes; see Abass, *supra* note 10, pp. 32-37.

and the Statute of the African Court pinpoints the possible ways of addressing the symbiosis between the ACC and the ICC based on the existing applicable laws of the two courts.

To do so, the article contains five sections. Following this short introduction the second section discusses the historical antecedents to the establishment of the ACC. The third section gives a general overview of the institutional design of the courts at the AU level. The different types of jurisdictional overlap that may arise between the ACC and the ICC are addressed in the fourth section, while section five examines the relationship between the ACC and the ICC. Under this part, the article explicates the different proposals forwarded by scholars to address the relationship between the ACC and the ICC. The flaws of the proposals are also highlighted in this part of the article. In addition, this part dwells on the complementarity regime of the ICC in light of the RCCs, particularly the ACC. Finally, the article wraps up by putting the threads together and forwarding sensible ways of addressing the relationship between the two courts based on their respective existing applicable laws.

## 2. Historical Background to the Establishment of the ACC

Several initiatives have been made to create the ACC that can investigate and prosecute perpetrators of international crimes in Africa. One of the pioneer attempts in this regard was done in the early 1970s.[32] The idea of creating an international criminal court for the prosecution of the crime of apartheid was begun during the discussions on the adoption of the International Convention on the Suppression and Punishment of the Crime of Apartheid in the early 1970s, but the proposal was not accepted during that time.[33] Following this, in 1981, during the discussion which paved the way for the adoption of the draft African Charter on Human and People's Rights the proposal for the establishment of a court to try violations of human rights and other international crimes was proposed by the government of Guinea. However, the idea was rejected

[32] Ademola Abass "Historical and Political Background to the Malabo Protocol" in Gerhard Werle and Moritz Vormbaum (eds), *The African Criminal CourtA Commentary on the Malabo Protocol* (Vol. 10, 2017 TMC Asser Press), p. 14; Marshet Tadesse Tessema *supra* note 24, p. 46; Max du Plessis, T. Maluwa and A. O'Reilly, "Africa and the International Criminal Court," *Chatham House International Law* Vol. 1, (2013), p. 9.

[33] Ademola Abass, *supra* note 32, p. 16. It is possible to conclude that the creation of the ACC was primarily inspired by the crimes of apartheid in South Africa, which was declared a crime against humanity by UN General Assembly in 1966.

because it was thought to be untimely.[34] Generally, the antecedents for the establishment of the ACC can be categorized into three.[35]These are first, abuse and misuse of Universal Jurisdiction by some European states.[36] The second triggering factor is the challenge and legal wrangling faced in bringing *Hissène Habré* to justice.[37] The third is the obligation imposed by the African Charter on Democracy, Election and Governance (ACDEG) to prosecute perpetrators of unconstitutional change of government before the competent court of the AU,[38] or in other words the existence of treaty obligation.

---

[34] Max du Plessis, T. Maluwa and A. O'Reilly *supra* note 32, p. 9; Marshet Tadesse Tessema *supra* note 24, p. 46.

[35] Ademola Abass *supra* note 32, p.15; Chacha Bhoke Murungu *supra* note 27, pp. 1068-1088; Max du Plessis, T. Maluwa and A. O'Reilly *supra* note 32, pp. 9-10; Charles Cheror Jalloh "The Place of the African Court of Justice and Human and Peoples' Rights in the Prosecution of Serious Crimes in Africa" in Charles C Jalloh, Kamari M Clarke and Vincent O Nmehielle (eds) *The African Court of Justice and Human and Peoples' Rights in Context: Development and Challenges* (1st edn, 2019, Cambridge University Press), pp. 74-88; Garth Abraham, *Africa's Evolving Continental Court Structures: At the Crossroads?*(South Africa's Institute of International Affairs (SAIIA) Governance and APRM Program, Occasional paper 209, 2015), p. 7.Available athttps://www.africaportal.org/publications/africas-evolving-continental-court-structures-at-the-crossroads/last visited September 2021; Marshet Tadesse Tessema *supra* note 24, p. 47; Ottili Anna Maunganidze and Anton du Plessis "The ICC and the AU" in Carsten Stahn (ed) *The Law and Practice of the International Criminal Court* (2015, Oxford University Press), p. 80.

[36] By invoking universal jurisdiction European states such as Belgium, France and Spain have issued arrest warrants against several sitting senior African officials, which were then challenged by African states and ruled as unlawful, hence abuse of universal jurisdiction, by the International Court of Justice. These misuses of universal jurisdiction served as one of the factors and cause which paves the way for the establishment of ACC. See generally, the Report of the Commission on the use of the Principle of Universal Jurisdiction by some non-African States as Recommended by the Conference of Ministers of Justice/Attorney General, the executive session EX.CL/411(XIII); Charles Chernor Jalloh, *Universal Jurisdiction, Universal Prescription? A Preliminary Assessment of the African Union Perspective on Universal Jurisdiction* (FIU Legal Studies Research Paper Series, Research Paper No. 17-28, 2017), p. 14; *Democratic Republic of Congo v Belgium* [2000] ICJ 121, [2000] judgment Para. 78 (2) (Arrest Warrant Case); *Belgium v Senegal* [2012] ICJ 24, judgment. Question relating to the obligation to Prosecute or extradite para. 16. (Question relating to the obligation to prosecute or extradite).

[37] To bring former Chad president *Habré* to book, it had to pass through different legal proceedings from ECOWAS Court, court of Belgium to ICJ. At the end, ICJ ruled that Senegal has duty to prosecute or extradite him to Belgium where he was wanted for serious crimes. This forced AU to come up with 'African solution for *Habré* problem'; given at the time there was a simmering tension between AU and the ICC. Besides, the *Habré* problem propelled AU to revive the ACC project and push the idea forward. For more on this see, Mbacke Fall "The Extraordinary African Chambers: The Case of Hissène Habré'' in Gerhard Werle, Lovell Fernandez and Mortiz Vormbaum (eds) *Africa and International Criminal Court* (Vol. 1, 2014, TMC Asser Press), p. 118; The decision on the Hissene Habre case and the African Union Doc. Assembly /AU/3(VII) 5 (ii). Assembly /AU/Dec.127(VII) In this decision, AU mandated the Republic of Senegal to prosecute and ensure that Hissène Habré is tried, on behalf of Africa, by a competent Senegalese court with guarantees for a fair trial; Decision on the Hissène Habré Case and the African Union, (Doc.Assembly/AU/8(VI)) Add.9, Assembly/AU/Dec.103 (VI), para. 2.( Decision on the Hissène Habré Case).

[38] African Union, African Charter on Democracy, Elections, and Governance (opened for signature 30 January 2007 entered into force 15 February 2012) Art.25(5).

The aspiration of establishing the ACC was revived and reinvigorated in 2009 when the AU Assembly requested that the AU, in consultation with the African Commission on Human and Peoples' Rights, and the ACHPR, "to examine the implications of the Court being empowered to try international crimes such as genocide, crimes against humanity and war crimes, and report thereon to the Assembly in 2010."[39] The immediate cause that necessitated the creation of the ACC within the existing African Court structure is the ICC's indictment of the then two sitting African Heads of State. The 2009 indictment of president Omar-Al-Basher of Sudan[40] is often considered the turning point for the deterioration of the relationship between the AU and the ICC. The subsequent commencement of investigation against Kenya's president, Uhuru Kenyatta, and deputy president, William Ruto has intensified this conflict.[41]

In the aftermath of the controversial presidential election, Kenya was plunged into widespread violence from 30 December 2007 to 28 February 2008.[42] The violence led to the death of more than 1,000 people, injury of 3,000 people, destruction of hundreds of thousands of homes and

---

[39] Assembly/ AU/Dec. 213 (XII) adopted at the 12th Ordinary Session of the Heads of State and Government Assembly in Addis Ababa, Ethiopia, from 1-3 February 2009, para. 9; African Union Assembly, Decision on the Report of the Commission on the Meeting of African State Parties to the Rome Statute of the International Criminal Tribunal (ICC), Assembly/AU/Dec.245(XIII) Doc. Assembly/AU/13(XIII) July 2009, Para 5; Ademola Abass *supra* note 32, p. 12; Marshet Tadesse Tessema, *supra* note 24, p. 47.

[40] Regarding the situation in Sudan, Darfur the case presented can be divided into four parts. The first is the case of former interior Minister Ahmad Muhammad Harun and former militia leader Ali Kushayb. In this case an arrest warrant was issued in May 2007. The second is the case of Darfur rebel leader BaharIdriss Abu Garda but the Prosecutor's case was dismissed by ICC judges in February 2010. The third case is related to Darfur rebel leaders Abdallah Banda, Abakaer Nourain, and Saleh Mohammed Jerbo Jamus pre-trial phase; charges confirmed in March 2011. The fourth case is related to Sudanese President al Bashir arrest warrant was issued in March 2009 for war crimes and crimes against humanity. One thing worth to mention at this juncture is additional arrest warrant is issued against the president for genocide in July 2010. For more on the issue of the case of Al Basher see Gerhad Kemp "Immunity of High- Ranking Officials Before the International Criminal Court-Between International Law and Political Reality" in Gerhard Werle and Andreas Zimmermann (eds) *The International Criminal Court in Turbulent Times* (Vol. 23, 2019 TMC Asser Press), pp. 61-82; Sascha Dominick Dov Bachmann, "The Africa Union-ICC Controversy Before the ICJ: A Way Forward to Strengthen International Criminal Justice," Washington International Journal, Vol. 29, No. 2, (2020), pp. 259 and following; see generally Elis Kepper, "Managing Set-backs for the International Criminal Court in Africa," *Journal of African Law*, (2011).

[41] Beth Van Schaack, *African Union and International Criminal Justice: where does it go from here? African Heads of State Before the International Criminal Court* (2015). Available at https://www.international-criminal-justice-today.org/arguendo/african-heads-of-state-before-the-international-criminal-court/last visited September 2021.

[42] David Anderson and Emma Lochery, "Violence and exodus in Kenya's Rift Valley, 2008: predictable and preventable?," *Journal of Eastern African Studies* Vol. 2, (2008), pp. 328–343.

buildings, and the forcible displacement of over 300,000 others.[43] The situation in Kenya marked the first *proprio motu* investigation initiated by the ICC Prosecutor for crimes committed on the territory of a State Party.[44] In this case, Uhuru Kenyatta who later becomes president and William Samoei Ruto who later became Vice President of Kenya charged with the commission of grave crimes during post-election violence between 2007 to 2008 including four other suspects.[45] However, the government of Kenya asked the UN Security Council to defer[46] the case against President Kenyatta and Deputy President Ruto on the ground that the indictment may pose a serious threat to the ongoing effort the promotion of peace, national healing and reconciliation, as well as the rule of law and stability, not only in Kenya but also in the region.[47]

Due to lack of sufficient evidence, the case against Ruto was terminated, similarly, charges against Kenyatta were withdrawn due to insufficient evidence. As the indictment of sitting Heads of state is unprecedented, it created a standoff between the AU and the ICC and created ripple effects across Africa. These two cases mounted the tension between the AU and the ICC which ultimately lead to the creation of the ACC within the existing African Court structure.

### 3. Structure of the ACC

As stated somewhere in this paper the African Court has three sections. Article 16 of the Merger Protocol of 2008 which reads 'Sections of the Court' is amended by Article 6 of the African Court Statute which reads 'Structure of the Court'. Accordingly, the African Court shall have

---

43 *Id*.

44 As required by the Rome Statute, the Prosecutor submitted an application for authorization to initiate investigations *proprio motu*, which was approved by a 2-1 vote. The case is against the then Politician William Ruto, Minister of Industrialization Henry Kosgey, and Journalist Joshua Arab Sang, Deputy Prime Minister Uhuru Kenyatta, Cabinet Secretary Francis Muthaura, and Maj. Gen. (Retd.) Hussien Ali. In this case the suspects voluntarily appeared before the Court in April 2011.

45 For more on the post-election violence in Kenya see generally Sosteness Francis Materu *The Post-Election Violence in Kenya Domestic and International Legal Responses* (Vol. 2, 2015 TMC Asser Press); Lionel Nichols *The International Criminal Court and the End of Impunity in Kenya* (2015 Springer International); David Anderson and Emma Lochery, *supra* note 42; Peter Kagwanja, "Courting Genocide: Populism, Ethno-Nationalism and the Information of Violance in Kenya's 2008 Post-Election Crisis, "*Journal of Contemporary African Studies*, Vol. 27, (2009), pp. 365-387.

46 Article 16 of the Rome Statute provides that "No investigation or prosecution may be commenced or proceeded with under this Statute for a period of 12 months after the Security Council, in a resolution adopted under Chapter VII of the Charter of the United Nations, has requested the Court to that effect; that request may be renewed by the Council under the same conditions."

47 Decision on International Jurisdiction, Justice and the International Criminal Court (ICC) Doc. Assembly/AU/13(XXI).

General Affairs, Human Rights and International Criminal Law Sections. According to Article 2 of the Malabo Protocol, the African Court has four major organs, namely the Presidency,[48] the office of the Prosecutor,[49] the Registrar,[50] and the Defence Office.[51]The ACC has three chambers namely, a Pre-Trial Chamber, a Trial Chamber, and an Appellate Chamber.[52] The Pre-Trial Chamber has powers to issue orders and warrants for the investigation and prosecution of cases, including protection of privacy of witnesses and victims, presentation of evidence and protection of arrested persons.[53] The Trial Chamber has the mandates to, among other things, conduct trials of accused persons and receives appeals from the Pre-Trial Chamber.[54] The Appeals Chamber receives and conducts appeals from the Trial Chamber.[55] To recap, the ACC exercise its jurisdiction over the 14 crimes through the instrumentality of its three chambers and the office of the prosecutor.

### 4. Jurisdiction of the ACC: Areas of Jurisdictional Overlap with the ICC

This section highlights the jurisdiction of the ACC and the plausible areas of jurisdictional overlaps between the ICC and the ACC. The potential jurisdictional overlaps between the ACC and the ICC, if and when the former becomes operational occur primarily in four facets of jurisdiction: territorial overlap, an overlap of jurisdiction concerning subject matters jurisdiction of the two courts, personal overlap (overlap of jurisdiction concerning perpetrators of the core crimes), and temporal overlap of jurisdictions. The other possible scenarios of jurisdictional overlap, albeit unlikely, are in the case of concurrent referrals by the AUPSC and the UNSC of the same situation to the ACC and the ICC, respectively; or when a non-party African state accepts the jurisdictions of the ACC and the ICC over the same situation. The following part dwells on these areas of jurisdictional overlaps between the two courts in an in-depth manner.

---

48 Art. 2 (3) of the Malabo Protocol. For more on the powers and functions of the presidency see Art. 22 of the African Court Statute.

49 Art. 2 (2) of the Malabo Protocol. For more on the function of the office of the prosecutor see Arts. 22A and 46G of the African Court Statute. The Office of the Prosecutor is envisaged by the Statute as one organ of the African Court, instead of as part of the ACC organ. This office has nothing to do with the other two sections so that it should have been placed under the structure of the ACC parallel to the three chambers of the later.

50 Art. 2(3) of the Malabo Protocol. For more see Art. 22B of the African Court Statute.

51 Art. 2(4) of the Malabo Protocol. For more see Art. 22C of the African Court Statute.

52 Art. 16(2) of the African Court Statute.

53 *Id*, Art. 19 Bis (2) and (3).

54 *Id*, Arts.18 and 19 Bis (4) and (5).

55 *Id*, Art. 19 Bis (6).

### 4.1. Territorial Overlap of Jurisdiction

Both the ACC and the ICC do not have universal jurisdiction. They both exercise jurisdiction based on certain grounds of jurisdiction. As far as their territorial jurisdiction is concerned they have jurisdictions over crimes committed within the territory of state parties.[56]As there are a substantial number of African countries, 33 to be precise, which are state parties to the ICC and would potential champion the ACC as well, there is an overlap of territorial jurisdiction between the ACC and the ICC. Unless the symbiosis between these two courts is addressed, this overlap of territorial jurisdiction would cause serious problems concerning the obligation of state parties towards the two courts. States will find themselves in a potentially conflicting obligation when both the ACC and the ICC request cooperation as regards the same situation or case.

### 4.2. Subject Matter Overlaps of Jurisdiction

The ICC has subject matter jurisdiction over four core crimes, namely genocide, crime against humanity, war crimes, and crime of aggression.[57]The ACC under Article 17(3) of the African Court Statute is empowered to hear cases specified in the Statute. In addressing the subject matter jurisdiction of the ACC, the Statute succinctly listed 14 crimes under the jurisdiction of the court. These are the four core crimes under the subject matter jurisdiction of the ICC and additional ten transnational crimes.[58] From these fourteen crimes under the jurisdiction of the ACC, the overlaps of subject matter jurisdiction with the ICC is as regards the four core crimes: genocide, crimes against humanity, war crimes, and aggression. As the definitions and elements of these crimes under the ACC statute are largely influenced by that of the Rome Statute[59] there is close to a total overlap of subject matter jurisdictions between the two courts as far as the four

---

56 Cf Art. 46Ebis and Art.12 (2) of the Rome Statute. It is worth mention that the ACC's bases of jurisdictions are broader than that of the ICC.

57 Art. 5 of the Rome Statute.

58 These crimes are genocide, crimes against humanity, war crimes, the crime of unconstitutional change of government, piracy, terrorism, mercenarism, corruption, money laundering, trafficking in persons, trafficking in drugs, trafficking in Hazardous wastes, illicit exploitation of natural resources, and the crime of aggression. See Art. 28A (1) of the African Court Statute.

59 Cf Art. 28B of the African Court Statute with Art.6 of the Rome Statute; Art.28C of the African Court Statute with Art.7 of the Rome Statute, Art.28D of the African Court Statute with Art.8 of the Rome Statute; and Art. 28M of the African court Statute with Art. 8bis of the Rome Statute.

crimes are concerned. Nonetheless, it is worth mentioning that the African Court Statute introduced some changes albeit minor to the elements of some of these core crimes.[60] In other words, there are trivial differences between the ACC and the ICC Statutes regarding definitions and objective elements of some of the core crimes. For instance, the Statute of the African Court under Article 28B (f) listed "acts of rape or any other form of sexual violence" as one objective element for the crime of genocide which is explicitly not included as an objective element of genocide under the Rome Statute. This addition by the ACC is not something novel because it had already been established in the jurisprudence of the International Criminal Tribunal for Rwanda (ICTR) that serious bodily or mental injury as one of the objective elements of genocide under the Genocide Convention covers acts like rape and other serious sexual violence.[61] Thus the explicit inclusion of rape and other sexual violence as one of the objective elements of genocide under the African Court Statute, other than clarifying the obvious, adds nothing to the scope of the material elements of genocide as known under the Genocide Convention and other instruments like the Rome Statute which are *telquel* copy of the former.[62] The reason behind such explicit inclusion in the African Court Statute is attributed to give emphasis to rape and other sexual violence as part of the crime of genocide.[63]

In addition, the Statute of the African Court also introduced additional *actaus rues* for war crimes such as disposition of the wounded, sick, shipwrecked, or dead; the use of nuclear weapons and other weapons of mass distraction[64] which are not included under Article 8 of the Rome Statute. Also, as regards recruitment of child soldiers as part of war crime, the African Court Statute raised the age to those under 18, which the ICC limited to children under 15.[65] Other than these minor differences as regards the objective elements of some of the core crimes

---

60 For instance, as regards recruitment of child soldiers as part of war crime, the African Court Statute raised the age to those under 18, which the ICC limited to those under 15. Cf. Art. 28D(xxvii) of the African Court Statute and Art. 8(2)(b)(xxvi) & 8(2)(c)(vii) of the Rome Statute.

61 *Prosecutor v Jean-Paul Akayeru,* [1999] ICTR-96-4-A, [1999] Judgment.Para.731; *Clement Kayishema and Obed Ruzindana* [1999] ICTR -95-1-T 21, [1999] Trial Judgment, para. 108; *Prosecutor v Radovan Karadic and Ratko Mladi* [1995] ICTR- IT-95-5-I, [1995] Indictment. para. 22; *Prosecutor v Radovan Karadic* [2016] ICTY-IT-95-5-18-T, [2016] Judgment, para. 545.

62 Kai Ambos "Genocide (Article 28B), Crime Against Humanity (Article 28C), War Crimes (Article 28D) and the Crimes of Aggression (Article 28M)" in Gerhard Werle and Moritz Vormbaum (eds) *The African Criminal Court a Commentary on the Malabo Protocol* (Vol 10, 2017, TMC Asser Press). P. 40

63 *Id.*

64 Art. 28D of the African court Statute.

65 Cf. Art. 28D(xxvii) of the African Court Statute and Art. 8(2)(b)(xxvi) & 8(2)(c)(vii) of the Rome Statute.

under the Statute of the African Court,[66] based on the foregoing discussion it is sound to conclude that there is an overlap of subject matter jurisdiction between the ICC and ACC as regards the four core crimes. Put otherwise, the overlap of subject matter jurisdiction between the ACC and the ICC, as things stand occurs only as regards the four core crimes. But as the Statutes of the two courts leave open the possibility to expand the subject matter jurisdictions of the Courts,[67]hence other areas of subject matter jurisdiction overlaps cannot be ruled out. Thus, in the future, when and if, states parties to the Rome Statute decide to expand the subject matter jurisdiction of the ICC to one or more of the ten additional crimes under the jurisdiction of the ACC through amendment of the Statute, jurisdictional overlaps other than the four crimes, may also arise.[68] For an amendment to the subject matter jurisdiction of the ICC to take place, the proposal of request for the amendment must be submitted to the United Nations Secretary-General who shall then promptly circulate the proposal to states parties.[69]A good example of this is the amendment made in Kampala which resulted in the adoption of additional objective

---

66 Pauline Martini, "The International Criminal Court *versus* the African Criminal Court A Remodeling of the Principle of Complementary as Solution to Potential Conflict of jurisdiction between the two courts," *Journal of International Criminal Law* (2021). For more on comparative study of the difference between the four core crimes under the ACC and the ICC, see Kai Ambos *supra* note 62, pp. 31-54; see also generally Eski Yemisi Ormoroge, "The Crimes of International Criminal Law in Africa: A Regional Regime in Response?," *Netherlands International Law Review,* (2019), pp. 287-309.

67 The African Court Statute explicitly states that 'the Assembly may extend up on the consensus of states parties, the jurisdiction of the court to incorporate additional crimes to reflect the development in international law', See Art. 28A (2). Although there is no such explicit provision in the Rome Statute, by using the amendment procedures provided in the same the states parties of the latter can also incorporate additional crimes. See Art. 121 (5) of the Rome Statute.

68 Road Rastan "Jurisdiction" in Carsten Stahn (ed) *The Law and Practice of the International Criminal Court* (2015, Oxford University Press), p. 147. In order to better explain the situation, Rastan mentioned some proposals that were made by some countries like "the proposal of Netherland to add 'the crime of terrorism' as new Art 5(e) and new Art 5(3) on the condition for the adoption and exercise of the crimes of terrorism (mirrored in the wording of former Art 5(2) concerning aggression), UN Doc C.N. 723.2009. TREATIES-5 (Depositary Notification); proposal of Mexico to amend to Art 8(2)(b) to include 'Employing Nuclear weapons or threatening to employ Nuclear weapons', UN Doc C.N.725.2009. TREATIES-5 (Depositary Notification); proposed amendment 2 and 3 by Belgium on behalf of Argentina, Belgium, Samoa, and Slovenia, to amend Arts 8(2) (b) and 8(2)(e) to include the use of biological and chemical weapons and anti-personnel mines, as well as the use of certain other weapons causing excessive harm, UN Doc C.N.733.2009. TREATIES-5 (Depositary Notification); proposal of Trinidad and Tobago to add 'The Crimes of International Drug Trafficking' as new Art.5(e) together with a proposed definition as new Art 5(2) concerning 'crimes involving the illicit trafficking in narcotic drugs and psychotropic substance when they pose a threat to the peace order and security of a state or region', UN Doc C.N. 737.2009.TREATIES-5 (Depository Notification)." See also 'United Nations Treaty Collection. Available at https://treaties.un.org/pages/AdvanceSearch.aspx?tab=UNTS&clang=_enlast visited September 2021.

69 Art. 121 of the Rome Statute. The Statute of the African Court does not have a detailed provision that regulate the amendment of the various parts of the Statute and the Protocol. See Art. 12 of the Malabo Protocol. There should have been a provision that clearly addressed the amendment procedures, decision-making and other related matters of the jurisdiction as well as other parts of the Statute and the Malabo Protocol.

elements for war crimes committed in the context of non-international armed conflict. The amendment extended the criminalization of the use of poisonous gases and bullets causing excessive suffering, which were only penalized when committed in an international armed conflict under Article 8 of the Rome Statute, to non-international armed conflict.

### 4.3. Personal Overlap of Jurisdiction

As regards personal jurisdiction, the ACC unlike the ICC which has jurisdiction only over natural persons[70] is empowered to exercise jurisdiction over artificial persons as well.[71] The personal jurisdiction of the ICC is based on the active personality principle, it can only exercise personal jurisdiction over nationals of states parties. Whereas, the grounds of personal jurisdiction of the ACC are not delimited to active personality. The ACC can assume jurisdiction based on not only the nationality of the perpetrators [72] but also the nationality of the victims (passive personality).[73] Thus the grounds for personal jurisdiction of the ACC are wider than that of the ICC. The personal jurisdictions of the ICC and the ACC potentially overlap over crimes perpetrated by the nationals of states parties to both the Rome Statute and African Court Statute. However, these overlaps might not occur as regards sitting heads of state and governments and other senior officials of African countries. The reason is, under the African Court Statute and before the ACC, sitting or incumbent Heads of State and Government and other senior officials are given immunity while they are in office. Article 46Abis of the Statute reads: "No charge shall be commenced or continued before the court against any serving AU Head of State or

---

70 Arts.1 and 25(2) of the Rome Statute.

71 Art. 46C of the African Court Statute. For more on corporate criminal liability under the ACC see Joanna Kyriakakis "Article 46(c) Corporate Criminal Liability of the African Criminal Court" in Charles C Jalloh, Kamari M Clarke and Vincent O Nmehielle (eds) *The African Court of Justice and Human and Peoples' Rights in Context: Development and Challenges* (1st edn, 2019, Cambridge University Press), pp. 793-835; see also Chantal Meloni "Modes of Responsibility (Article 28N), Individual Criminal Responsibility (Article 48B) and Corporate Liability (Article 46c)" in Gerhard Werle and Moritz Vormbaum (eds) *The African Criminal Court a Commentary on the Malabo Protocol*, (Vol. 10, 2017, TMC Asser Press), pp. 151-154; Evelyne OwiyeAsaala "Corporate Criminal Liability Under the Malabo Protocol: Breaking new ground?" in HJ Van der Merwe and Gerhard Kemp (eds) *International Criminal Justice in Africa (2017)* ( 2018, Strathmore University Press ), pp. 107-127; Joanna Kyriakakis, *Corporate Criminal Liability at the African Criminal Court Briefing Paper* (ACRI Meeting 2016).

72 Art 46 E bis 2(b) of the African Court Statute.

73 Art 46E bis 2(c) of the African Court Statute.

Government, or anybody or entitled to act in such capacity, or other senior state official based on their functions, during their tenure of office."[74]

This provision is contrary to what Article 27 (1) of the Rome Statute provides. The latter does not recognize immunity to anyone including sitting Heads of State and Governments. Some writers argue that the immunity provided under the African Court Statute is unacceptable and is a retrogressive step in the development of international criminal law but this matter is not within the ambit of this article. [75]

### 4.4. Temporal Overlap of Jurisdiction

The Statute of the African Court, as well as the Rome Statute, has limited temporal applications of their respective Statute and thereby the jurisdictions of the courts to the time after entry into force of their respective founding instruments.[76] Both courts are forward-looking, instead of retrospective courts. In the case of the ICC, as the Rome Statute entered into force in July 2002, in principle it can exercise jurisdiction over crimes committed after this period. As regards, the ACC, it is yet to garner the minimum ratification requirements for it to enter into force. At the time of writing, an overlap of temporal jurisdictions between, or other facets of jurisdiction for that matter, the ACC and ICC, is a non-issue. Under the Statute of the African Court the Court is empowered to exercise its jurisdiction 30 days after the amended court had entered into force.[77]Thus, an overlap of temporal jurisdictions between the ICC and ACC will arise only over crimes committed after the entry into force of the Malabo protocol and the Statute of the African Court.

---

74 Art. 46Abis of the African Court Statute.

75 See Marshet Tadesse Tessema *supra* note 24, p. 35; Mia Swart and Karin Krisch, "Irreconcilable Differences? An Analysis of the Standoff between the African Union and the International Criminal Court," *African Journal of International Criminal Justice* Vol. 1, (2014), p. 48.

76 Art. 11(1) of the Rome Statute; Arts.11 of the Malabo Protocol and Art. 46E of the African Court Statute; see also Erika De Wet,*supra* note 29, p. 187.

77 Art. 46E(2) of the African Court Statute.

### 4.5. Jurisdictional Overlaps in Case of Referrals by the UNSC and the AUPSC

One of the trigger mechanisms for the jurisdiction of the ACC and the ICC is referrals of crimes committed in the territory of a non-party state, by the AUPSC and UNSC, respectively.[78] The other possible area of overlap between the ACC and the ICC is in cases where both the UNSC and the AUPSC make referrals of the same situation to the ICC and the ACC respectively. As indicated under Article 13(b) of the Rome Statute, one of the triggering mechanisms of the ICC's jurisdiction is the referral of the situation by the UNSC. This provision enables the ICC to undertake investigation and prosecution in states not a party to the Rome Statute following the UNSC referral. The Statute of the African Court under Article 46F (2) also vested the AUPSC with the competency to refer cases to the ACC. Both the UNSC and the AUPSC can make a referral of the same situation to the ICC and the ACC, respectively, albeit unlikely, that can give rise to an overlap of jurisdiction between the two courts.

### 4.6. Jurisdictional Overlaps in Case of Ad hoc Acceptance of Jurisdiction

Although the obvious jurisdictional overlaps between the ACC and the ICC occur in the case of the above-highlighted facets of jurisdictions, there is also another possible potential area of overlap of jurisdiction. This is when a non-party African state accepts the ACC and the ICC jurisdiction over the same situation. A non-party state can create a jurisdiction for the ACC and ICC to which they could otherwise be not entitled by a declaration of ad hoc acceptance of jurisdiction.[79] By way of simultaneous ad hoc acceptance of ACC's and ICC's jurisdiction, a non-party state may create jurisdictional overlaps between the two courts. Although this kind of overlap of jurisdiction is rare, it can be considered one potential area of jurisdictional overlap between the ACC and the ICC.

## 5. Complementarity Principle of the ACC and the ICC

The Rome Statute as well as the Statute of the African Court recognizes the complementarity principle as a means to regulate their respective relationship with national criminal jurisdictions. The provision of the ACC that regulates the complementarity principle is substantially

[78] Cf. Art. 46F of the African Court Statute and Art 13 (b) of the Rome Statute. As can be discerned for the Article 46F (2) of the African Court Statute the Assembly of Heads of State and Government of the African Union' also has the power to refer a situation to the Office of the Prosecutor of the African Court/the ACC.

[79] See Arts. 12, 13 (a) and 14 of the Rome Statute and Art 46Ebis (3) of the African Court Statute.

influenced by Rome Statute. Simply put, the ACC's complementarity principle largely replicates the complementarity provision of the ICC. The principle of complementarity is based on two basic pillars: respecting state sovereignty, on one hand, and ending impunity, on the other hand. In other words, based on the principle of complementarity, states maintain primary jurisdictions over perpetrators of even the most heinous crimes while the ICC and the ACC are courts of last resort vis-à-vis national criminal jurisdictions. In the part that follows, this section examines whether the principle of complementarity by extension can also help address the possible relationship between the ACC and the ICC.

### 5.1.Complementarity Principle of the ICC

The principle of complementary is considered one of the pillars of the Rome Statute.[80] At the heart of the principle of complementarity is the idea that states have the priority to investigate and prosecute perpetrators of core crimes. Article 17 of the Rome Statute lists the grounds which make a case inadmissible before the ICC. These parameters are complementarity tests that ensure that the ICC does not compete with national criminal jurisdictions. These are:

a) If "the case is being investigated or prosecuted by a State which has jurisdiction over it, unless the State is unwilling or unable genuinely to carry out the investigation".
b) If "the case has been investigated by State which has jurisdiction over it and the State has decided not to prosecute the person concerned, unless the decision resulted from the unwillingness or inability of the State genuinely to prosecute";
c) If "the person concerned has already been tried for conduct which is the subject of the complaint, and trial by the Court is not permitted under article 20, paragraph 3 of the Statute"; and
d) If "the case is not of sufficient gravity to justify further action by the Court."

Although the parameter for evaluating the phrase "case being investigated" under article 17(1)(a) is not clear the ICC tried to elaborate the meaning through different case laws. Accordingly, the

[80] Preambular paragraph 10 of the Rome Statute vividly states that "the International Criminal Court established under this Statute shall be complementary to national criminal jurisdiction", and Art. 1 echoes this. In addition to this Art.17 (1) of the Rome Statute refers to preambular paragraph 10 and to Art. 1. In addition to this in *Prosecutor v Joseph Kony, Vincent Otti, Okot Odhiambo and Dominic Ongwen case* the Pre-Trial Chamber II, while deciding on admissibility of the case under article 19(1) of the Statute described complementarity as "one of the cornerstones of the Rome Statute, see *Prosecutor v Joseph Kony, Vincent Otti, Okot Odhiambo and Dominic Ongwen* [2009] ICC-02/04-01/05-377-10, [2009] Pre-Trial Chamber II decision, para. 34.

ICC interpreted the phrase "case being investigated" under article 17 (1)(a) by using the "same person same conduct" test.[81]

To determine whether a case is inadmissible because of unwillingness article 17(2) lists three types of unwillingness that the court must consider: the first type of unwillingness is that national procedures were or are being used to shield a person from criminal responsibility; the second type of possible unwillingness is if there has been an unjustified delay in the proceeding, showing a lack of intent to prosecute; and the third unwillingness is if the independence and impartiality of prosecuting institutions cannot be guaranteed.

Another element of complementarity in the Rome Statute is inability. Article 17(3) lists grounds for determination of inability. Accordingly, in order to determine inability in a particular case, "the Court shall consider whether, due to a total or substantial collapse or unavailability of its national judicial system, the State is unable to obtain the accused or the necessary evidence and testimony or otherwise unable to carry out its proceedings."

The word "genuinely" under article 17(1)(a) presupposes that the action taken by the state should be real and sincere. To evaluate the gravity threshold under article 17(1)(d) the court should take into account qualitative and quantitative considerations, such as the scale, nature, manner of commission, and impact of the crimes.[82]

---

[81] *Prosecutor v. Ahmad Muhammad Harun and Ali Muhammad Ali Abd-Al-Rahman*, [2007] ICC-02/05-01/07-l Corr, [2007] Pre-Trial Chamber I, Decision on the Prosecution Application under Article 58(7) of the Statute, para. 24; *Prosecutor v. Germain Katanga*, [2007] ICC-01/04-01/07-55 [2007] Pre-Trial Chamber I, Decision on the evidence and information provided by the Prosecution for the arrest of Germain Katanga, para. 20; *Prosecutor v Germain Katanga*, [2009] ICC-01/04-01/07-1497 OA 8 [2007] Oral Decision of the Trial Chamber II of 12 June 2009 on the Admissibility of the Case, paras 81-82; *Prosecutor v. Thomas Lubanga Dyilo*, [2006] ICC-01/04-01/06-8-US-Corr [2006] Pre-Trial Chamber I, Decision on the Prosecutor's Application for a warrant of arrest, para. 31; *Prosecutor v. Kony et al*., [2009] ICC-02/04-01/05-377 [2009] Pre-Trial Chamber II, Decision on the Admissibility of the Case under Article 19(1) of the Statute, paras 17–18; *Prosecutor v. Francis Kirimi Muthaura et al*., [2011] ICC-01/09-02/22-96 [2011] Decision on the Application by the Government of Kenya Challenging the Admissibility of the Case Pursuant to Article 19(2)(b) of the Statute, para. 48; and *Prosecutor v. William Samoei Ruto et al*.,[2011] ICC-01/09-01/11-101 [2011] Decision on the Applicability by the Government of Kenya Challenging the Admissibility of the Case Pursuant to Art 19(2)(b) of the Statute, para 54.

[82] *Prosecutor v. Bahar Idriss Abu Garda* [2010] ICC-02/05-02/09-243-Red [2010] Decision on the confirmation of charges, para. 31; *Situation in the Republic of Cote d'Ivorie,* [2011] ICC-02/11-14-Corr, [2011] "Corrigendum to Decision to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Republic of Côte d'Ivoire, paras. 203-204; see also article 37 of Office of the Prosecutor Policy paper on case selection and priortisation 2016.

Generally, a given case is admissible before the ICC only if a state is inactive, unwilling, or unable to investigate and /or prosecute the perpetrators of the core crime/s.[83] In other words, the ICC may exercise jurisdiction over a case only when states fail to genuinely investigate and /or prosecute those who have committed horrendous international crimes. The Rome Statute provides a good framework for determining whether the national justice system is unwilling or unable to genuinely investigate and/or prosecute perpetrator/s of core crime/s.[84]

### 5.2.Complementarity Principle of the ACC

The Statute of the African Court also by stipulating the complementarity principle succinctly recognizes that the ACC is a supplementary court to national criminal jurisdiction.[85] The provisions of the Statute of the African Court that deal with complementarity are modelled after the complementarity provisions of the Rome Statute. Nevertheless, there are some significant variations. The ACC complements not only national courts but also Regional Economic Communities (RECs). At present time there are no RECs that have jurisdiction over international crimes; however, if, in the future, the jurisdiction of RECs is expanded and RECs are empowered with the power to investigate and prosecute international crimes, the ACC would not compete with such RECs.[86] This is because the African Court Statute has already in anticipation

---

83 Art. 17 (2) of the Rome Statute.

84 For more on complementarity, admissibility and inadmissibility tests of the Rome Statute, see Jo Stigen *The Relationship between the International Criminal Court and National Jurisdictions the Principle of Complementary* (Vol. 14, 2008, Martinus Nijhoff Publishers), pp. 251-330;Werle, G/Jessberger, F *Principles of International Criminal Law*, (3 edn, 2014, Oxford University Press: Oxford), pp. 103 and following; Stahn C and El Zeidy, MM (eds) The International Criminal Court and Complementarity: From Theory to Practice (2011, Cambridge University Press: Cambridge); Ova Catherine Imoedemhe *The Complementary Regime of the International Criminal Court National Implementation in Africa* (2017, Spring International Publishing), pp. 32-39; Sascha Dominik Dov Bachmann and Eda Luke Nwibo, ''Pull and Push'-Implementing the Complementary Principle of the Rome Statute of the ICC within the AU: Opportunities and Challenges," *Brookly Journal of International Journal of Law,* Vol. 43, (2018), pp. 484-490. For detailed discussion on same and for more relevant materials see Triffterer, O /Ambos, K *The Rome Statute of the International Criminal Court: A Commentary* (3 ed, 2016, Hart Publishing: Oxford), pp. 781 and following.

85 Preambular, para. 17 of the Malabo Protocol; and Art 46H of the African Court Statute. The Statute vividly states that the jurisdiction of the court "shall be complementary to that of the National Courts and to the Courts of the Regional Economic Communities where specifically provided for by the Communities."

86 In this regards Margaret states that "another layer of complexity will be added to the complementary analysis, particularly in case where states, RECs, and the ACC have overlapping jurisdiction" Margaret M. Deguzman "Complementary at the African Court" in Charles C Jalloh, Kamari M Clarke and Vincent O Nmehielle (eds)

addressed the relationship between the ACC and RECs, by making the former complementary to the latter.

Likewise, the ICC's complementarity, the schemes of complementary principles under the ACC become operational by applying admissibility criteria to the case. The admissibility criteria affirm the fact that states are the ones with primary rights (and by extension duty) to investigate and prosecute perpetrators of crimes. Consequently, inhibits the ACC from interference when states are carrying out investigations and/ or prosecutions in accordance with the complementarity parameters. In other words, the ACC should intervene only when either of the admissibility parameters is present, otherwise, the case should be inadmissible before the ACC. The inadmissibility criteria of the ACC are similar to that of the ICC.[87] Thus, the ACC shall determine a case inadmissible where: (a) a case is being investigated by a State provided that the State is willing and able; (b) the State investigated the case and genuinely decided not to prosecute; (c) the person has been tried for conduct which is the subject of the complaint, or (d) if the ACC finds the case of not sufficient gravity. Put differently, a case is admissible before the ACC only if the state is inactive, unwilling or unable.

Therefore, neither the ACC nor the ICC is competing for courts with national courts, they complement national courts. Consequently, the duty to investigate and prosecute perpetrators of international and/or transnational crimes is primarily the responsibility of states. The ACC and the ICC step up to investigate and prosecute crimes under their respective jurisdictions only when states fail to conduct adequate/genuine investigation and prosecution.

There are some differences between the ACC's complementary provisions and that of the ICC. The first difference is the omission of the qualifier "genuinely" from Article 46H 2(a) and (b) of the African Court Statute.[88] The reason provided for the omission of the qualifier concerning

---

*The African Court of Justice and Human and Peoples' Rights in Context: Development and Challenges* (1st edn, 2019, Cambridge University Press), pp. 647 and 648; Ademola Abass, *supra* note 32, p. 25.

87 Cf. Arts 46H of the African Court Statute and Art. 17 of the Rome Statute. For more see, Marshet Tadesse Tessema, *supra* note 24, p. 54.

88 Margaret M. Deguzman *supra* note 86, p. 648 and 649; Harmen van der Wilt "Complementary Jurisdiction (Article 46H)" in Gerhard Werle and Moritz Vormbaum (eds) *The African Criminal CourtA Commentary on*

investigation or prosecution is that state leaders were unwilling to grant the ACC the power to gauge the genuineness of their respective national criminal proceedings.[89] Some writers strongly argue that the absence of the word "genuinely" from the Statute of the African Court renders the provision absurd.[90] The absence of the qualifier genuinely to "inability to prosecute" will lower the evidentiary standard of inability and will make the African States reluctant to prosecute perpetrators of crimes before courts. This may thereby excessively saddle the ACC with enormous cases turning it into a court of first rather than last resort.[91]

Other authors argue that the absence of the qualifier "genuinely" from the Statute of the African Court does not cause a serious problem and does not have substantial consequences. The reason is "if the investigation or prosecution by a concerned State is not genuine, it still can be considered as unwilling, based on the parameters provided in the Statute."[92]

The second difference between the ACC's complimentary provisions and that of the ICC is that under the Rome Statute there is a provision dealing with the ways to challenge the jurisdiction of the Court.[93] However, the Statute of the African Court does not incorporate Rome Statute's counterpart on issues of challenging the jurisdiction or admissibility of the case before the ACC. This should have been addressed appropriately. Nonetheless, it does not mean that it is not possible to challenge the ACC's jurisdiction.[94] Be this as it may, the complementarity principle of both the ACC and the ICC does not address their interaction; the issue then is: what their symbiosis is? The part that follows dwells on this.

---

*the Malabo Protocol* (Vol. 10, 2017, TMC Asser Press) p. 192; Marshet Tadesse Tessema, *supra* note 24, p. 55 and Ademola Abass, *supra* note 32, p. 26.

89 Margaret M. Deguzman, *supra* note 86, pp. 648 and 649.

90 *Id*.

91 Ademola Abass, *supra* note 32, p. 25.

92 Marshet Tadesse Tessema, *supra* note 24, p. 55.

93 Art 19 of the Rome Statute.

94 The Court is empowered to enact different rules of procedures including rules of procedure that regulate appeal from decisions of the Pre-Trial and Trail Chamber.

## 6. Complementarity Principle as a Panacea to Jurisdictional Overlaps between the ACC and the ICC

As discussed under section three of this article, the ACC and the ICC have overlapping jurisdiction albeit tangentially. According to the principle of complementarity, states remain the primary enforcers of international criminal law. Both the ICC and the ACC are courts of last resort; they are established to complement national criminal jurisdictions.[95]

The rationale behind the complementary principle under the ICC as well as the ACC is to strike the balance between state sovereignty, on one hand, and filling the impunity gap, on the other hand. According to this principle, neither the ICC nor the ACC is courts set up to supplant or compete with the national jurisdiction system.

Both the ACC and the ICC are established by multilateral treaties. However, there is no single provision in the Statutes of the two courts that address their relationship with one another. One reason suggested by writers regarding the failure of the Rome Statute to regulate its relationship with regional criminal courts like the ACC is that at the time when the Rome Statute was adopted there was no REC entrusted to prosecute perpetrators of the core crimes.[96]

The Rome Statute as a forward-looking treaty should have anticipated such a possibility and explicitly addressed its symbiosis with RECs. Regrettably, the Statute of the African Court does not even mention the ICC even though 33 African countries are parties to the Rome Statute. The Statute of the African Court as it was adopted way after the Rome Statute should have included a provision that regulates the relationship of the ACC with the ICC. The absence of a clear provision that regulates the relationship between the two courts is regrettable.

Scholars advanced different proposals on the possible ways of addressing the relationship between the ACC and the ICC. The solutions advanced for the problem include amendment of

---

95 Marshet Tadesse Tessema *supra* note 24, p. 54; Robert Cryer and others *An Introduction to International Criminal Law and Procedure* (2007 Cambridge University Press), p. 153 and Jo Stigen *supra* note 83, p. 2.

96 Marshet Tadesse Tessema, *supra* note 24, p. 56; Harmen van der Wilt, *supra* note 87, p. 191; and Margaret M. Deguzman *supra* note 86, p. 672.

the Rome Statute to recognize regional complementarity;[97] others developed a relationship based on a hierarchical or cooperative method;[98] others invoked the principle of pendency as a way to resolve the jurisdictional overlap.[99] However, these proposals are not free from defects. This section provides a general overview of the different proposals advanced by other scholars, highlights their defects and attempts to come up with viable ways to regulate the symbiosis between the ACC and ICC based on the existing applicable laws of these courts.

As regards the option of rectifying the Rome Statute to recognize regional complementarity,[100] in October 2013, in an extraordinary session the AU adopted a Draft Decisions on Africa's relationship with the ICC. In this Draft Decision regarding the relationship between the ACC and the ICC, the AU recommended that African states members of the Rome Statute introduce an amendment to the Rome Statute to recognize the establishment of regional arrangement with international criminal jurisdiction per the principle of complementarity.[101] However, this language was changed in the final resolution of the AU session, which decided that "African

---

97 Draft Decision on African's Relationship with the International Criminal Court (ICC), 12 October 2013, Page. 9; Konstantinos D Mogliveras, "Substituting International Criminal Justice for an African Criminal Justice?," *International Organizations Law Review,* Vol. 14, (2017), p. 310; see also Amnesty International, *"Malabo Protocol: Legal and Institutional Implications of the Merged and Expanded African Court Snapshots,"* (2016), p. 22. Available at https://www.amnesty.org/en/documents/afr01/3063/2016/en/last visited September 2021.

98 Harmen van der Wilt *supra* note 88, pp. 195-202.

99 Pauline, acknowledging the existence of overlap of jurisdiction between the two courts and the corresponding conflict, and came up with the concept of "first refusal". See Pauline Martini, *supra* note 66, p. 8. According to first refusal "the Court investigating or prosecuting a case in the first instance has primary jurisdiction over that case, to the exclusion of the other Courts". This concept is based on the principle of pendency. The principle of pendency states that if a case is pending before one court, no other court shall try any case in which the matter in the issue is directly and substantially similar to the one before another court. If the state which has primary responsibility to investigate and prosecute perpetrators of the core crimes becomes inactive and if the ICC steps in to investigate and prosecute first it ousts the jurisdiction of the ACC thereby excluding the ACC. This solution is not something novel and can stand as a solution by itself. The reason being this is already covered by the complementarity principle. The complementarity principle of the Rome Statute gives priority to investigate and prosecute heinous crimes to states concerned. If a state fails to investigate or prosecute a case the one which starts the investigation either the ACC or the ICC first, excludes the other. Generally, this is covered by the complementarity principle. But what needs to be questioned and clarified is whether the principle of pendency in criminal matters has extraterritorial applicability.

100 On regional complementarity, see, Miles Jackson, "Regional Complementarity: The Rome Statute and Public International Law," *Journal of International Criminal Justice,* Vol. 14, (2016).

101 Draft Decision *supra* note 97, Page. 9; Konstantinos D Mogliveras, *supra* note 97, p. 310; Amnesty International, *supra* note 97, p. 22.

States parties propose a relevant amendment to the Rome Statute, per article 121 of the Statute."[102]

Accordingly, Kenya proposed an amendment to the preambular paragraph of the Rome Statute on 7 November 2013 as follows: "Emphasizing that the International Criminal Court established under this Statute shall be complementary to national and regional criminal jurisdiction."[103] At present, the Preamble reads, "Emphasizing that the International Criminal Court established under this Statute shall be complementary to national criminal jurisdictions."[104] Nevertheless, this proposal has not got the needed support. Thus, this seems not a workable solution for the current issue at hand.

The other proposal regarding the relationship between the ACC and the ICC is the one developed by Harmen van der Wilt. Harmen proposes two models for the future relationship between the ACC and the ICC which requires amendment of the Statutes of the courts to regulate the relationship between the two courts. The first approach is based on a hierarchical model; the second is based on a cooperative model.[105]The hierarchical model is based on the selection and division of cases. According to this model, the ICC is empowered to prosecute grave core crimes while leaving others less grave to the ACC.[106] According to Harmen if prosecution by the ACC does not meet the standard measurements of the ICC this may be tantamount to the inability or unwillingness of the ACC and this may become the sufficient ground to warrant activation of the jurisdiction of the ICC over the case.[107] The problem with this approach is first it is hardly possible if not impossible to determine the meaning of gravity. Second, this kind of hierarchical

---

102 Decision on Africa's Relationships with the international criminal court (ICC), Ext(Assembly/AU/De. 1/Oct. 2013), Par. 10 (VI).

103 Report of the working group on amendments, ICC-Adp/13/31, 7 December 2014, 17; African Union Withdrawal Strategy, Draft 2 Version 12 January 2017, 9. Available at https://www.hrw.org/sites/default/files/supporting_resources/icc_withdrawal_strategy_jan._2017.pdf last visited September 2021.

104 Preambular paragraph 10 of the Rome Statute.

105 Harmen van der Wilt, *supra* note 88, pp. 195-202.

106 *Id*, p.199.

107 *Id*, p.191.

relationship does not exist between international courts.[108] In other words, it is unlikely for African states or any other continent to concede to such relegation of the institution they created.

The second approach which is the cooperative model is based on a division of labour based on the category of crimes, then gravity as such. In this approach, the ICC will try the core four international crimes and the ACC will have jurisdiction over the transnational crimes.[109] Again, this seems untenable as it is clearly against the very intention of the African heads of state and government. [110] The latter proposal is not as such a way of resolving the jurisdictions' overlap but rather a sort of striping the ACC of some of its subject matter jurisdictions. In simple terms, both proposals presuppose agreement between the ICC's Assembly of States Parties and African countries on the apportionment of jurisdictions between the two courts over cases where they exercise concurrent jurisdiction.[111]It is far from reality to expect such an agreement between the creators of the courts; thus, these proposals are not viable ways to address the interaction between the two courts.

The other option to regulate the relationship between the ACC and the ICC is perhaps their complementarity principle. The complementary principle of the Rome Statute regulates the relationship between states and the Court. As mentioned somewhere in this article, the Rome Statute does not mention or regulate its relationship with the RCCs like the ACC. However, by advancing a teleological interpretation of the applicable laws of the ICC it is possible to advance that the spirit of the complementarity principle of the ICC accommodates not only the establishment of regional arrangements but also their primacy jurisdiction that can be justified for three strong reasons.

---

108 *The prosecutor v Tadic* [1995] ICTY -IT-94-1-AR72, [1995] Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Appeals Chamber para. 11. In this Case, the International Criminal Tribunal for the Former Yugoslavia held that; "International law, because it lacks a centralized structure, does not provide for an integrated judicial system operating an orderly division of labor among a number of tribunals, where certain aspects or components of jurisdiction as a power could be centralized or vested in one of them but not the others. In international law, every tribunal is a self-contained system (unless otherwise provided)."

109 Harmen van der Wilt, *supra* note 88, p. 196.

110 Pauline Martini, *supra* note 66, p. 8.

111 *Id*.

First, the complementarity principle of the ICC expressly addresses the relation between states and the ICC. States can exercise their primary responsibility of bringing perpetrators of the core crimes before justice acting on an individual basis or they can exercise their primary responsibility collectively by delegating the power of investigation and prosecution of the perpetrators of the core crimes to regional arrangements. States create a regional arrangement by granting part of their sovereign right to prosecute atrocity crimes to that regional entity to act on their behalf. In other words, states cannot create institutions and empower them with the power that states themselves do not have or cannot exercise. The African states even those who are parties to the ICC can exercise their entitlement (and duty) to investigate and prosecute by using their national courts or by empowering regional arrangements to do the same on their behalf. Thus the writers strongly argue that the ICC complements not only domestic courts but also the RCCs like the ACC. Thus RCCs in general and the ACC particularly should be considered as an extension of national jurisdictions.

Second, the experience of the International Military Tribunal at Nuremberg (IMTN) clearly shows that international law does not hinder two or more states from creating an *ad hoc* tribunal with criminal jurisdiction to try perpetrators of atrocity crimes on their behalf. Thus, as the primary aim of the complementarity principle is to fill the impunity gap, prosecution by states concerned or by duly constituted RCCs should be equated to prosecution by national courts. Thus, it is possible to argue that the complementarity principle while expressly regulating the relationship between the ICC and national courts by extension recognizes the right of states to establish regional arrangements with international criminal jurisdiction.

Lastly, it is a trite fact that human rights systems are regionalized through the adoption of regional human rights treaties. Currently, there are three most well-established regional human rights systems, namely in Europe, Latin America and Africa. Regionalization of human rights enforcement systems is presumed to be helpful to deal with the particular human rights concern of a given region and it has strengthened human rights protection. Akin to regionalization of the human rights system, regionalization of international criminal justice should be seen positively and encouraged as it helps to address the distinctive conditions, needs and concerns of a given region. Studies established that there have been 80 coups and 180 attempted coups between 1956

and 2001 in Sub- Saharan Africa.[112] Outside of Africa, unconstitutional change of government is a rare phenomenon. Unconstitutional change of government and other similar crimes are of concern for the African continent, not as such of concern to other regions. The establishment of RCCs like that of the ACC helps to deal with such cases of specific relevance to a given region, in this case, Africa. Thus, the establishment of such an arrangement should be considered progressive and a step in the right direction for the development of international criminal law.[113] Consequently, "… a genuine criminal prosecution by a lawfully constituted regional tribunal means that the 'case is being…prosecuted by a state which has jurisdiction over it' for the purpose of Article 17(1)(a)."[114]

Generally, it can be argued that African states created the ACC by seeding part of their sovereignty. The RCCs in general and the ACC, in particular, should be considered as an adjunct to the ICC rather than competing Courts. Accordingly, genuine prosecution by a lawfully constituted regional tribunal should be equated with prosecution by the state party concerned. In case when the ACC is inactive, unwilling or unable to investigate and prosecute perpetrators of crimes the ICC can step in to investigate and prosecute perpetrators of the core crimes to fill the gap of impunity.[115]

## 7. Concluding Remarks

The amendment to the Protocol on the Statute of the African Court of Justice and Human Rights established a tripartite court structure by merging the General Affairs Section, the Human and Peoples' Rights Section and the ACC into a single court—African Court. The crimes under the subject matter jurisdiction of the ACC are a mixture of the four core crimes under the jurisdiction of the ICC and ten transnational crimes. There are 33 African states which are parties to the ICC; consequently, the ICC has jurisdiction over the core crime/s committed in the territory of these countries or perpetrated by nationals of the same. This creates an overlap of jurisdiction between the ACC and the ICC concerning the four core crimes.

---

112 Stef Vandeginste, "The African Union, Constitutionalism and Power-Sharing," *Journal of African Law*, Vol. 57, (2013), p. 2.
113 Miles Jackson, *supra* note 100, p.1062.
114 *Id*.
115 Harmen van der Wilt, *supra* note 88, p. 196.

The overlap of jurisdiction between the ACC and the ICC has taken the focus of much attention. However, writers have not come to a consensus regarding the possible ways of addressing the relationship between the ACC and the ICC. This article analyzed the applicable laws of the two courts to pinpoint the plausible ways to address the (potential) jurisdictional conflict between the two courts.

The article concludes that the spirit of the complementarity principle under the ICC accommodates the establishment of RCCs in general and the ACC in particular. Thus, the ACC should be considered an adjunct to the ICC and the latter should not be considered a competing court. The ICC is complementary not only to national criminal jurisdictions but also to the ACC. By advancing a such teleological interpretation of the applicable laws of the courts, it is sound to argue that the two courts can co-exist as supplementary institutions. The ICC can fill the impunity gap and supplement the ACC, by investigating and prosecuting incumbent Heads of State and Government and other senior government officials who perpetrated core crimes but enjoy immunity before the ACC.

The establishment of RCCs like the ACC should be supported and promoted. This kind of regional arrangement helps to deal with crimes of specific relevance and concern to a respective in which they operate. RCCs like the ACC enrich the international justice landscape and they are additions to the menu of accountability options available for prosecution of perpetrators of international and transnational crimes. Thus, the AU and African countries should promote the ratification of the Malabo Protocol and the Statute to operationalize the ACC.

# Global-Regulation of Cyberspace Security and the Ethiopian Context

Fikreselassie Getachew*

**Abstract**

*Cyberspace has become an emerging target of invisible actors thereby calling for strict regulation of cyberspace a global agenda. Recently globe with embroiled with rising state-sponsored cyberattacks resulting in a diminishing trust and confidence among states. The vast and disruptive nature of cyberspace coupled with its anonymity creates a new and effective way for nations to pursue their national interest against their adversaries with great deniability and fewer consequences. Global effort toward regulating states' behavior within cyberspace is largely hampered by geopolitical tensions and disagreements between various countries. Despite continued global dialogues toward developing norms and new international laws capable of regulating state-sponsored cyberattacks, the world is still without a comprehensive and binding agreement that can restrain global peace and security threats. The article explores the ongoing global cybersecurity regulatory debates in line with its impact on Ethiopia's cybersecurity capability.*

Keywords: Cyberspace, Cybersecurity, Cyberattack, Cybercrime, Cybernorms, State Actors, Critical Infrastructure

## 1. Introduction

With the ever-expanding technological advancement global cyber-threats have been increasing extensively in alarming rate. According to the World Economic Forum 2020 Global Risk Report, technology-related risks, specifically, cyberattack risk ranked 7th among the major catastrophes that could potentially endanger global peace and security in the coming 10 years.[1] Apart from the threat, cybercrime poses to the peace and security of the international community cyber-attacks have been causing adverse economic and social effects across the globe. Based on the Assessment of Cybersecurity Venture, the global damage arising out of cybercrime is expected to grow by 15 percent per year, thereby costing 10.5 trillion USD annually by 2025.[2]

*LL.B., LL.M.

1 WORLD ECONOMIC FORUM, THE GLOBAL RISKS REPORT 2020 12, (15th ed. 2020).

2 Steve Morgan, Cybercrime Magazine*, Cybercrime to Cost the World $10.5 Trillion Annually By 2025*, (Mar. 27, 2022, 09:30 AM), https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/).

Currently, a growing number of states are developing new policies and institutions for the political and military application of cyberspace.[3] We are witnessing phenomena whereby the number of ICT-related incidents involving nation-States is increasing both in number and sophistication.[4] Even though large-scale state-sponsored cyber-attacks are relatively a recent phenomenon, there are accounts of major state-sponsored cyberattacks that undermine trust between governments. Considering cyberattacks can originate in any part of the world, it is difficult for any single nation to adequately deal with cyberattacks, highlighting the need for an urgent and comprehensive international response. To this end, numerous states and international organizations embarked on making multifaced efforts to reduce the risks associated with the malicious use of ICT. Despite the efforts and ongoing dialogue, the world is yet to come up with a comprehensive agreement regarding the means and methods of regulating cyberspace. There are still unresolved questions at the global level regarding how the existing international law should be shaped and regulate responsible States' behavior within the cyber realm.[5]

Currently, only a handful of States (mostly European and the USA) have begun to express their position on the issue while the vast majority of nations including Ethiopia remain silent and inactive in the process.[6] Nations with strong cyberspace infrastructure and. Knowhow have started launching different initiatives that can potentially influence other nations toward setting new norms and rules in the field of cyberspace. Consequently, States weak and vulnerable infrastructure are facing an ultimatum in siding with stronger nations without properly scrutinizing the issue on their terms.

The extent of cybersecurity issue and continues threat that Ethiopia has been defending has increased in alarming rate. According to the 2020/2021 fiscal year national cybersecurity report, Ethiopia has encountered 2,800 reported cyberattack attempts targeting several institutions and key infrastructures.[7] The number of attacks recorded this year is more than double what has been

---

3 Vladimir Radunović, *Cybersecurity and International Peace and Security*, https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Summary-International-Peace-and-Security.pdf. (Aug. 19, 2021, 11:15 PM).

4 UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, THE UNITED NATIONS, CYBERSPACE AND INTERNATIONAL PEACE AND SECURITY: RESPONDING TO COMPLEXITY IN THE 21ST CENTURY 9 (2017).

5 Duncan B. Hollis, *A Brief Primer on International Law and Cyberspace,* (Aug. 4, 2021, 10:08 PM), https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763. Same as above

6 See *Id*.

7 *Id.*

recorded in the previous 2019/2020 fiscal year (1080) showing the extent of the cyber incident growth in the country. According to Ethio-CERT, [2] the law enforcement operation that is being held in the northern part of the country, the second filling of the GERD, as well as the sixth national election were all responsible for the increasing number of cyber-attacks during the fiscal year.[8]

In the current northern Ethiopia conflict between the federal government and Tigray forces, cyberspace is being actively used by domestic and international actors to influence the outcome of the war. The apparent disinformation and misinformation campaign against the country through social media is hurting the social development and stability of the country as well as the psychology of its citizens. In line with the current information warfare, social media accounts of major Ethiopian institutions like Ethiopian Broadcasting Corporation and Ethiopian Airlines were recently hacked as part of this coordinated campaign. In this Hybrid type of warfare against Ethiopia, informational warfare tools are being deployed together with another wide array of powerful diplomatic, political, economic, and military tools by internal and external forces to weaken Ethiopia's national unity, security, and global influence.[9] Recently misinformation, fake news, and hate speech deployed within cyberspace coupled with willful and deliberate misinformation campaigns of western-backed mainstream media are becoming an existential threat to the country. Hence, the impact of information-based cyber warfare is becoming a well-anticipated and recognized threat to Ethiopia that needs to be addressed through a coordinated effort of multiple stakeholders.

Apart from the current disinformation campaign, another emerging challenge within cyberspace is those targeting the country's critical infrastructures. According to the head of Ethio-CERT, [2] one of the most prominent and persistent groups targeting Ethiopian cyberspace is hacker groups who call themselves the "Cyber Horus Group."[10] The group, supposedly affiliated with the Government of Egypt, was responsible for the attack on 37, 000 computers and government-associated websites between June 17-and 20, 2020.[11] These attacks ware coincided with the second filling of GRED

---

[8] Seblewoyne, *supra* note 68

[9] Interview with Hannibal Lemma, Division Head, Cyber Governance and Management Division, Information Network Security Agency (Jan 4, 2022).

[10] Seblewoyne, *supra* note 68.

[11] Addis Zeybe, **'***Cyber Horus' hacking group mounts cyberattack on 37,000 computers in connection with Grand Ethiopian Renaissance Dam,* (Jan.9, 2020, 1:45PM), https://addiszeybe.com/featured/currentaffairs/technology/cyber-horus-hacking-group-mounts-cyberattack-on-37-000-computers-in-connection-with-grand-ethiopian-renaissance-dam.

and the escalating tension between Ethiopia and Egypt. The ultimate aim of the attack was to create confusion around the filling and operation of the dam and to put pressure on Ethiopia over its dispute with Egypt. During this attack, the hacking group attempted to attack several public service institutions, and private companies including some security agencies' websites, and try to disrupt the operation of certain critical infrastructures.[12]

Even though there is a lack of concrete evidence that links the hacker group with Egypt, the timing and the motives of the attacks coupled with pharaonic-themed nationalistic messages left by the hacker group raised suspicion as to who could be behind these attacks. The plausible deniability that is inherent to the anonymity of cyberspace crate makes it difficult to ascertain a cyber-attack by a particular threat actor. However, if proper cybersecurity measures are not taken, this sort of cyber-attack demonstrates the magnitude of the challenge that cyberspace poses in the future by providing fertile ground for different state and non-state actors. This goes to show how the cyber domain is being exploited by domestic as well as international adversaries to pursue their political and military agenda against Ethiopia.

Despite these national security threats Ethiopia's cybersecurity capability is still facing different challenges. Recent audits and evaluations conducted in 2020 among 61 institutions demonstrate that a lack of cybersecurity awareness; limited priority afforded to cybersecurity; absence of cybersecurity management and administration procedure; lack of cybersecurity technology; and lack of cybersecurity regulatory frameworks account for most of the cybersecurity vulnerability in Ethiopia.[13] Even if the cyber incidents that are being reported are increasing substantially, most of these incidents targeting Ethiopia were averted before causing significant harm to the country.[14] However, considering most critical infrastructures of the country and essential government services are recently starting to deploy and integrate ICT services, the impact of cybersecurity vulnerability would be a significant threat to national security.[15]

This article examines the ongoing global cybersecurity regulatory debate and its implication for Ethiopia's future cybersecurity capability by applying the traditional doctrinal research

[12] See *Id.*
[13] Cybersecurity Audit Report, Information Network security Agency /unpublished/2020.
[14] Seblewoyne, *supra* note 68.
[15] Hannibal, *supra* note 73.

methodology. The article briefly explores the current cybersecurity measures and global cooperative efforts made by the Ethiopian government together with their challenges.

## 2. Cyberspace and State-Sponsored Cyberattacks

The fourth Industrial revolution has introduced fast processing and large-scale machine-to-machine communication stirring up major social, political, cultural, and economic changes.[16] These large-scale communication capabilities together with higher computing power prompted the creation of a more connected, complex, and strange new domain called Cyberspace. More recently, cyberspace is being considered the fifth operational human domain being added to the four well-established domains like land, sea, air, and space.[17] Even if there are several meanings attributed to the word cyberspace,[18] it is widely understood as an abstract world or alternative environment enabled by the internet and computer.[19]

One of the unique characteristics of Cyberspace is that it does not have a physical or geographical border as it exists and plays a major role in all of the other existing domains.[20]Unalike natural areas (air, sea, land, and space) cyberspace is not- territorial,[21] it is an omnipresent domain available to anyone in the globe where the internet is accessible. Because of this, cyberspace provides an opportunity for any individuals or groups with the necessary skill-set to execute cyberattacks in any dimension anonymously with limited or no risk of being caught. This character of cyberspace makes it difficult to attribute a certain malicious cyber incident or attack to a specific individual, organization, or state making the new domain a threat to national and international peace and security.

Cyberspace provides giant neighborhoods as well as the world's largest battlefield. It affects the operation of governments, the military, small businesses, corporations as well as the lives of almost every individual on the planet. As long as the internet exists and people continue to use computing

---

16 CHRISTINA BOGUSZEWICZ and et. Al, THE FORTH INDUSTRIAL REVOLUTION AND CYBERSPACE'S MENTAL HEALTH STIGMA 2 (2020).

17 Dan Efrony, *The Cyber Domain, Cyber Security and what about the international law?* (Aug. 20, 2021, 12:09 AM) https://csrcl.huji.ac.il/sites/default/files/csrcl/files/dan_efrony.pdf.

18 Lance Strate, *Cyberspace: The Varieties of Cyberspace: problems in definition and delimitation,*63(3) W.J. Co 383 (2009).

19 Riza Azmi and Kautsarina, *Revisiting Cyber Definition*, (Aug. 20, 2021, 2:27 PM) https://www.researchgate.net/publication/334989724_Revisiting_Cyber_Definition/link/5d5a18ca299bf151badeb164/download.

20 Dan, *supra* note 8.

21 Lino Santos, *Cyberspace regulation: Cesurists and Traditionalists*, 6(1) E.jo.Int. Re. 88 (2015).

devices in their personal and professional capacity there will be an underline concern originating from cyber threats and cyber-attacks. In the current technological landscape having entirely secure software from errors and bugs is impractical, making software flaws the underlying factor for most cybersecurity breaches. Cyber-attacks can occur whenever a threat actor identifies, analyzes, and exploit these software vulnerabilities for his/her benefit. Even though different descriptions can be attributed to cyberattacks, they are an attack initiated from a computer against a website, computer system, or computer that compromise the confidentiality, integrity, or availability of the computer or information stored on it.[22] Cyberspace facilitates an effective way of conducting many human conducts including crime. With sufficient know-how cybercrimes are easy to commit and hard to detect as compared to traditional crime,[23] thereby making cybercrimes a more dangerous and contemporary threat to global communities. Cybercrime has been adversely impacting the economy, social values, cohesion, and democratic assets.

The complex nature of cyberattacks attributed to their limitless realm of existence makes cyberspace an emerging global threat. This nature of cyberattacks coupled with its anonymity creates a new and effective opportunity for states to pursue their national interest agendas against their rivals with great deniability and fewer consequences. Even though technology influenced the outcome of conventional warfare since the first computer systems came into the picture, the utilization of cyber warfare as an alternative is a relatively new phenomenon. The introduction of weapons of mass destruction /WMD/ makes direct military confrontation between countries with WMD capability obsolete. As a result, developed States are actively working toward enhancing their technological capabilities to engage in cyber warfare to continue advancing their political, economic, and military interests without resorting to conventional warfare.

In light of these developments, global communities have been witnessing large-scale state-sponsored cyberattacks, that have the potential to cause significant and wide-ranging harm across several critical assists.[24] The most prominent and alarming state-sponsored cyber sabotage or

---

[22] Vince Farhat & ET AL, *Cyber Attacks: Prevention and Proactive Responses,* (Aug. 21, 2021, 3:36 AM) https://www.academia.edu/3785382/Cyber_attacks_preventative_proactive_responses.

[23] Vijaykumar S. Chowbe, *The Concept of Cyber-Crime: Nature & Scope,* (Aug. 21, 2021, 11:06 AM) http://ssrn.com/abstract=1766238.

[24] Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376 (2018).

disruption are cyberattacks targeting other states' critical infrastructure.[25] Critical infrastructures (CI) are the physical and non-physical resources and services that are fundamental to the minimum functioning of a society.[26] The infrastructures are crucial in ensuring public welfare, economic stability, law enforcement, and defense operations.[27] The extensive integration of ICT into CI increases CI's vulnerability and makes them a target of malicious attacks via cyberspace.[28] Hence, any attack campaign targeting CI can have a significant impact on the national security of any nation, contributing to diminishing trust and confidence among states.

Currently, some state-sponsored major cyberattacks on critical infrastructure which resulted in global tension and outcry. Estonia was the first country in the world to face a coordinated cyber-attack against its critical infrastructures. Following Estonian government decisions to reallocate soviet era war memorial, in May 2007 Estonian government networks were heavily harassed by Distributed Denial of Service /DDoS/ attack by foreign intruders (allegedly attackers associated with the Russian Government).[29] Over three weeks, Estonia's government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses were all crippled by unprecedented levels of internet traffic.[30]In an event widely regarded as the first major act of cyber warfare in the world, Estonia lost productivity, opportunity cost, remediation, and the acquisition of alternative web hosting at emergency rates estimated to be in the billions of Euros.[31]

The dialogue of cyber warfare resurfaces again in 2010 when researchers discovered Stuxnet, a resilient computer worm that damages the nuclear centrifuges in Iran.[32] Stuxnet forced the control systems of the Iranian nuclear centrifuges to spin out of control while preserving the appearance of proper function for the controllers.[33] The actor behind Stuxnet has not been identified officially.

---

25 Vijaykumar, *supra* note 14.

26 Viganò, Eleonora & ET AL, *Cybersecurity of Critical Infrastructure, in* THE ETHICS OF CYBERSECURITY 157, 158. **(**Markus Christen et al. eds., 2019).

27 See *Id*.

28 *Id.*

29 Center For Strategic and International Studies, *Significant Cyber Incidents Since 2006,* (Aug. 24, 2021, 12:38 AM), https://csis-website-prod.s3.amazonaws.com/s3fs-public/210804_Significant_Cyber_Events.pdf? bzKYK94rq5 _ 3lrbYVK4fcL0rmkNq6lNI. See also Ministry of Defense Cyber Security Strategy Committee, Estonia Tallinn 2008 EE_NCSS_2008_en.pdf (last accessed July 23, 2022).

30 Andreas Schmidt, *The Estonian Cyberattacks*, *in* THE FIERCE DOMAIN –CONFLICTS IN CYBERSPACE 1986-2012 52, 52 (Jason Healey ed.,2013).

31 *Id.* at 53.

32 JAY P. KESAN AND HAYES CAROL M. HAYES, CYBERSECURITY AND PRIVACY LAW IN A NUTSHELL 2 (2019).

33 See *id.*

However, depending on the code size, complexity, and development efforts behind this lethal weapon, many sources strongly believe it to be a joint effort by the United States of America and Israel.[34] Stuxnet is considered to be the first well-known demonstration of the cyber attacker's ability to harm physical infrastructure.[35] Apart from attacks targeted toward critical infrastructures States meddling in the internal affairs of opponent States is becoming a new global security agenda. This form of intervention was witnessed when Russia allegedly set out to interfere with the 2016 US election. Throughout the election wide range of politically damaging information on the internet was released on social media platforms that can influence the outcome of the election. The US considers this meddling in the 2016 election as an attack on its national interest and its democratic values, making the country respond with hefty diplomatic and economic sanctions.

Currently, these international cyber incidents are not slowing down, as can be inferred from the recently deteriorating US-China relation in cyberspace.[36] Unfortunately, the difficulty of identifying cyber attackers and their motivations in cyberspace resulted in the Nations States classifying all serious cyberattacks as cyberwar.[37] This imminent cyber threat and agitations fuel a cyberwar arms race, resulting in more instability and less security around the world.[38] Hence, with increased cyberwarfare capabilities around the world, no single country is safe from cyber-attacks.

### 3. International Law and Cybersecurity

In recent years, the idea of global cyberspace governance as an operational domain has been gathering momentum from various state and industry actors. The complexity of cyberspace opens up a bunch of new and difficult legal issues like whether existing bodies of international law apply to cyberspace or not. In the current context, this open question surrounding the application of international law to cyberspace is entangled with disagreement among major geopolitical rivals. The geopolitical rivalry between the US and its allies on one hand and Russia and their allies emanate from their domestic policy toward regulating and utilizing cyberspace. The west advocate

---

[34] Siddharth P. Rao, *Stuxnet - A new Cyberwar weapon,* (Aug. 24, 2021, 2:18 AM), https://www.researchgate.net/ publication /267156195_Stuxnet_A_new_Cyberwar_weapon_Analysis_from_a_technical_point_of_view.

[35] See *id.*at 3.

[36] Ariel (Eli) Levite and Lyu Jinghua, *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?* (Mar. 27, 2021, 03:10 PM), https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213

[37] Bruce Schneier, *Cyberconflicts and National Security,* https://www.un.org/en/ chronicle/article/ cyberconflicts-and-national-security. (Accessed Aug. 24, 2021, 9:54 AM)

[38] *Id.*

cyberspace to be a domain that is an open, interoperable, secure medium that preserves the free flow of information globally.[39] The west is resistant to the enactment of a new international law that in any way control/censors the contents of cyberspace.

Contrary to the West's assertion, the group led by Russia and China promotes more controlled and regulated cyberspace whereby state sovereignty is well respected[40] and advocates for the creation of stricter rules of responsible state behavior in the cyberspace. To this end, Russia for the first time proposed a draft UN resolution in 1998 to establish a new and binding international law dealing with cybersecurity.[41] Russia and a handful of other states also submitted a proposal for a voluntary International Code of Conduct for Information Security in 2011 to re-affirm their long-standing position.[42] On the contrary, the western states categorically reject the idea of a new international legal framework regulating cyberspace and advocate for the development of norms as to how the existing international laws can be applied to cyberspace. Accordingly, international legal experts primarily from the Western Hemisphere developed the Tallinn Manual to serve as an international standard that can bring some degree of clarity to the complex legal issues surrounding the application of international law for cyberspace.[43] These Manuals address many international laws issue related to state cyber operations including general international law as well as specialized international law regimes like human rights, diplomatic laws, the law of the sea, air law, space law, and more.[44]

Nowadays, the issues of cyberspace regulation has become the agenda of the globe.[45] The regulation of information security /cyberspace security/ has been a hot discourse of the UN since 1998 after the Russian Federation had introduced a draft resolution on the subject in the First Committee of the UN General Assembly.[46] The request at the time was based on the assertion of the Russian government that new technologies could be used for purposes that are not compatible

---

[39] Elaine Korzak, Russia's Cyber Policy Efforts in the United Nation, 11 Tallinn Paper, 4, 20 (2021).
[40] See *id.*
[41] *Id* at 5.
[42] *Id* at 7.
[43] Eric Talbot, *The Tallinn Manual 2.0: Highlights and Insights,* 48 Geo. Jo. Int. Law 738, 736 (2017).
[44] See *id.*
[45] Ma Xinmin, *Key Issues and Future Development of International Cyberspace Law,* 2(1) Ch.Q.Int.St.S., 119, 120 (2016).
[46] United Nation, *Developments in the field of information and telecommunications in the context of international security*, (Aug. 25, 2021, 8:43 PM), https://www.un.org/disarmament/ict-security/.

with the objectives of international peace and security. This Russian initiative contributed to situating Nation-States cyber conduct as a global security issue for the first time. This Russian proposal on the issue of technology and its implications for global security face strong opposition mostly from western nations led by the US. However, it has gained enough support among other UN members to be included on the UN global security agenda.

Since the first Russian initiative, efforts of formulating international law for global cyberspace security have already been continuously proposed and contested by different international actors. Currently, global legislative development concerning cyberspace is largely influenced by different specialized institutions under the UN, regional actors, specialized international organizations, and governments and stakeholders from different states.[47]

### *3.1. UN Based Efforts Towards Global Cyberspace Security*

Since the last two decades, the UN General Assembly (UN GA) has been pushing for a global dialogue to draw a line between responsible and irresponsible state behavior toward cyberspace. While noting the potential use of ICT for malicious purposes, Cybersecurity has become the agenda for the UN GA for the first time in 1998. Through Resolution 53/70 the UN GA decided to include development in the field of information and telecommunication in the context of international security.[48] After having several backs and forth forward and debates between the Western states and the Russian Federation, Russia's proposal for the establishment of a Group of Governmental Experts (GGE) to study the matter was endorsed.[49]

In 2003 through Resolution 58/32 The GA requested the Secretary-General (SG) to conduct a study on relevant international concepts aimed at strengthening the security of the global information telecommunication system with the assistance of a GGE to be established in 2004.[50] This Resolution triggered the establishment of the first GGE to examine the impact of technology on international peace and security.[51]Since then UN GA has adopted several Resolutions to convene five other GGEs and one Open-Ended Working Group (OEWG) to further develop norms that can

---

47 Abid A. Adonis, *International Law on Cyber Security in the Age of Digital Sovereignty* (Aug. 27, 2021, 06:20 PM), https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/

48 U.N. GA, 53th Sess., 79th plen. mtg. at 2, U.N. Doc. A/RES/53/70, (Dec. 4,1998).

49 UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, *supra* note 4, at 15.

50 U.N. GA, 58th Sess., 71th plen. mtg. at 2, U.N. Doc. A/RES/58/32, (Dec. 8,2003).

51 Digwatch, *UN GGE and OEWG*, (Aug. 27, 2021, 2:58 AM), https://dig.watch/processes/un-gge.

help assure international cyber stability. These groups were created to discuss different key issues under the areas of information security identified by the General Assembly and the Secretary-General of the UN. These key issues include existing and emerging threats; norms, rules, and principles of responsible behavior of states; confidence-building measures; international cooperation and assistance in ICT security and capacity building, how international law applies to the use of ICTs, conclusions, and recommendations for future work.[52]

### *3.2. The Group of Governmental Experts*

The first GGE was established in 2004 following the term of resolution 58/32 composed of experts from 15 states.[53]Taking into its mandate and the various reports submitted from the Member States, the Group had a comprehensive and in-depth exchange of views among its members on the field of cybersecurity.[54] However, the Group failed to reach consensus in the preparation of the final reports due to geopolitical tension between Russia and the USA. Considering the Group operates based on consensus the dissent of the US and its allies from the final report was enough to prevent the report from being issued. The second GGE was established in 2009 to continue studying the existing and potential threats in information security and possible cooperative measures to be taken. Unlike the first GGE, the second Group produced the first consensus report after a comprehensive exchange of views. The group identified threats, risks, and vulnerabilities associated with ICT and suggested confidence-building steps to be taken to mitigate the risk associated with cyberspace.[55] Even though the Group delivered a consensus report it failed to deliver on one of the tasks it set out to do concerning how international law applies to the use of ICT.

Building upon the 2010 report of the second GGE, the third GGE produced the second consensus report.[56] This was considered as one of the most successful Groups establishing the relevance of international law to cyberspace.[57] The report reflects the Group's finding that international law, in particular the United Nations Charter, is "essential in […] promoting an open, secure, peaceful, and

---

[52] Katherine W. Getao, *The Value of International Cooperation in Cyberspace; Lessons from the UNGGE Processes,* (Aug. 28, 2021, 5:51 PM), https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-03.pres_ungge_lessons_for_africa_katherine_g_.pdf.
[53] U.N. GA, 60th Sess., at 2, U.N. Doc. A/60/202 (Aug. 5,2005).
[54] See *id.*
[55] U.N. GA, 65th Sess., at 6, U.N. Doc. A/60/202 (July. 30,2010).
[56] U.N. GA, 68th Sess., U.N. Doc. A/68/98, at 6 (Jun. 13,2013).
[57] Katherine, *supra* note 43.

accessible ICT environment."[58] Similar to the third Group, the fourth GGE produced the third consensus report reaffirming the 2013 third GGE stand that international law in particular the UN Charter, applies to states' use of ICT[59]. In addition to reaffirming this stand, the 4th Group further considered how international law applies to the use of ICTs by states. However, the most important milestone achieved by this Group was the adoption of 11 voluntary, non-binding norms for responsible states' behavior. [60]These norms guide nations to: [61]

- cooperate toward increasing the stability and security in the use of ICT and preventing harmful ICT practices;
- consider all relevant information in case of ICT incidents;
- not knowingly allow their territory to be used for internationally harmful ICT acts**;**
- consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICT;
- ensure the secure use of ICTs, to guarantee full respect for human rights, including the right to freedom of expression;
- not conduct or knowingly support ICT activity; that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure;
- take appropriate measures to protect their critical infrastructure from ICT threats;
- respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts;
- take reasonable steps to ensure the integrity of the supply chain, so end users can have confidence in the security of ICT products;
- encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities;
- not conduct or knowingly support activity to harm the information systems of another State's authorized Computer Emergency Response Team (CERT).

---

58 U.N. GA., *supra* note 47.
59 U.N. GA, 70th Sess., at 12, U.N. Doc. A/70/174 (July. 22,2015).
60 See *id*. at 7and 8.
61 UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, *supra* note 4, at 19.

The fifth Group was established by GA Resolution 70/243 with 25 experts to continue to study similar issues that have been specified in the GGEs.[62] However, during the discussion, of the Group significant differences in position and interest between states emerged regarding the means of applying the rules of international law to states' use of ICT.[63] Because of these differences, the Group failed to deliver a consensus report. The 6th GGE was established by GA Resolution 73/266. It successfully produced the 4th consensus report to the GA. The 2021 GGE, despite the occurrence of exceptionally high tensions between key players due to hostile cyber operations targeting GGE members, achieved consensus.[64] One of the major achievements of the Group was building up the eleven voluntary, non-binding norms developed by the fourth GGE report, and developing an additional layer of understanding of these norms.[65] The report underscored the value of these 11 norms and further developed their substantive contents by adding commentary on their meaning as well as the kind of institutional arrangements. [66]The other important milestone achieved by this Group was the acknowledgment that international humanitarian law (IHL) applies to cyber operations during an armed conflict.[67]

### *3.3. The Open-Ended Working Group*

The UN GA through Resolution 73/27 established an Open-Ended Working Group (OEWG) in which all Member States are invited to participate. This group was created based on a Russian proposal to find a new way of re-engaging in the global information security negotiation that will avoid the group agreements created by the UN GGE.[68] Nonetheless, at the time, many delegations expressed their frustration with the creation of UN OEWG for discussion, which they considered as having a similar mandate to the UN GGE.[69] Unlike the GGE in which only a limited number of states participate, the OEWG was established to create more democratic, inclusive, and transparent

---

62 U.N. GA., 70th Sess., 82nd plen. mtg. at 3, U.N. Doc. A/RES/70/237, (Dec. 23,2015).
63 UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, *supra* note 4, at 19.
64 Michael Schmitt, The Sixth United Nations GGE and International Law in Cyberspace, (Aug. 28, 2021, 6:15 PM), https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.
65 U.N. GA, 76th Sess., at 8, U.N. Doc. A/76/135 (July. 22,2015).
66 See *id.*
67 See *id.* at 18.
68 A surprising turn of events: UN creates two working groups on cyberspace, (Jan. 1, 2022, 3:15 PM), https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/
69 See *id.*

groups that work on a consensus basis.[70]Accordingly, it opens the door for all states to participate express their views, and extend cooperation on cybersecurity.

The group was tasked to further develop the rules, norms, and principles of responsible behavior in the field of information and telecommunication in the context of international security. The Group was also allowed to hold consultative meetings with interested parties (business, non-governmental organizations, and academia). Following its mandate, the OEWG discussed the existing and potential threats in cyberspace and possible cooperative measures to address them and produce its report in March 2021.[71] The Group's Report is built on a framework already established in the previous GGE reports. Aside from further elaborating and commenting on these issues, the most important achievement of the OEWG was the engagement of a large number of UN members and other non-governmental actors who were ready to collaborate and contribute to the global cybersecurity agenda.

## 4. Ethiopian Cybersecurity Landscape

Since the last decade, Ethiopia has been working to place ICT within the wider context of its socio-economy development agenda and reap the potential benefit it has in terms of sustaining development. The Ethiopian government for the first time recognizes ICT as one of its strategic priorities with the adoption of the National ICT Policy in 2011.[72] This policy document demonstrates the government's commitment to developing ICT both as an enabler of socio-economic development as well as an industry on its own. The policy lays down the road map for transforming the country from a subsistence agricultural-based economy to a knowledge and information-based economy.

Since the approval of the first National ICT Policy, the government of Ethiopia has made several attempts to promote ICT as one of its strategic priorities in its national development plans. These government endeavor has been manifested in the adoption of the first and second Growth and Transformation Plan (GTP) and the 2016 updated national ICT policy. Currently, consistent with the 2019 Home Grown Economic Reform Agenda, the Government is implementing the 10-year

[70] U.N. GA., 73th Sess., 45th plen., at 5, U.N. Doc. A/RES/73/27, (December 5,2018).
[71] U.N. GA., at 2, Doc. A/AC.290/2021/CRP.2, (March 10 2021)
[72] FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA, THE NATIONAL INFORMATION AND TECHNOLOGY POLICY AND STRATEGY 1 (2011).

development plan and the Digital Ethiopia 2025 digital strategy to further embrace technology across all core development sectors to build a digital economy. To this end, the Ethiopian government recently has made several changes including its longstanding policy of opening up the telecommunications sector for the private sector to lay the foundation for future digital transformation. All advances and initiatives launched in the past couple of years toward mainstreaming digital technologies into the broad national development context resulted in the expansion of ICT infrastructure and access to technology across the country.

According to the Ethio Telecom 2021/2022 fiscal year first-half business performance report (as of 31st December 2021), its total subscribers reached 60.8 million.[73] Meanwhile, Ethio Telecom is currently running several projects on infrastructure and system capacity expansions to boost network coverage capacity and quality of services.[74] Similarly, the same report indicates exponential growth in mobile subscribers accounted for 96.5% of the overall subscription. In the same period fixed broadband access surged to 443,000 from 347,000 in just six month period, while a total of 23.8 million 'Data and Internet' users at the end of the reporting period.[75] This report indicates a fourfold increase in subscriptions from the 2010/2011 fiscal year.[76] Even though it is still underdeveloped as compared to other developing countries, the expansion of ICT infrastructure and the ever-growing access to technology in Ethiopia has profound implications for development as well as a new form of cyber threats.

### *4.1. National Cybersecurity Challenges*

Ever since the country has centered ICT into its wider socio-economic development context the country has increasingly become dependent on the vast and global cyberspace domain. Accordingly, as reliant of computer technology, Ethiopia has been facing the security challenges that strung along with being part of cyberspace. Simply put, due to the ever-increasing dependency and accessibility of technology we are witnessing an increasing number of cyber-attacks that are becoming a challenge to the socio-economic development and stability of the country. Cyberspace

---

[73] Ethio telecom 2014 EFY (2021/22) First Half Business Performance Summary Report, (Apr. 16, 2022, 04:21 AM) https://www.ethiotelecom.et/የኢትዮ-ቴሌኮም-የ2014-በጀት-ዓመት-የመጀመሪያ/

[74] See *id.*

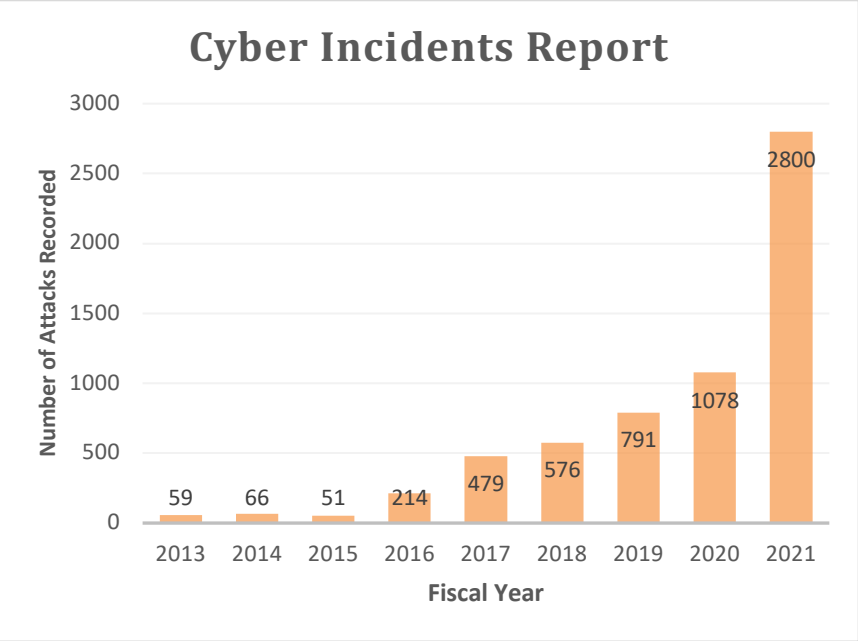
[75] See *id*

[76] Comms Update*, Ethio Telecom reveals financial results, subscriber data for most recent financial year*, (Nov. 25, 2021, 10:44) https://www.commsupdate.com/articles/2011/09/15/ethio-telecom-reveals-financial-results-subscriber-data-for-most-recent-financial-year/.

has been actively exploited recently by different extremists, terrorists, criminal groups as well as nation-states to advance their interests against the country, making it a new source of national security threat.

Even though the number of cyber-attacks is still relatively low as compared to other developing countries,[77]reports coming out of the Information Network Security Agency /INSA/ indicate these numbers are exponentially increasing in recent years. Ever since INSA start reporting Ethiopia's annual cyber security incident in 2013, evidence suggests an increasing number of cyber-attacks are targeted toward Ethiopia.[78] Accordingly, the 59 /fifty-nine/ cyber-attacks registered in 2013 have increased more than 47-fold to 2800 (one thousand seventy-eight) cyber incidents in 2021.

Figure 1. **INSA Cyber Incidents Report (between 2013 and 2021)**



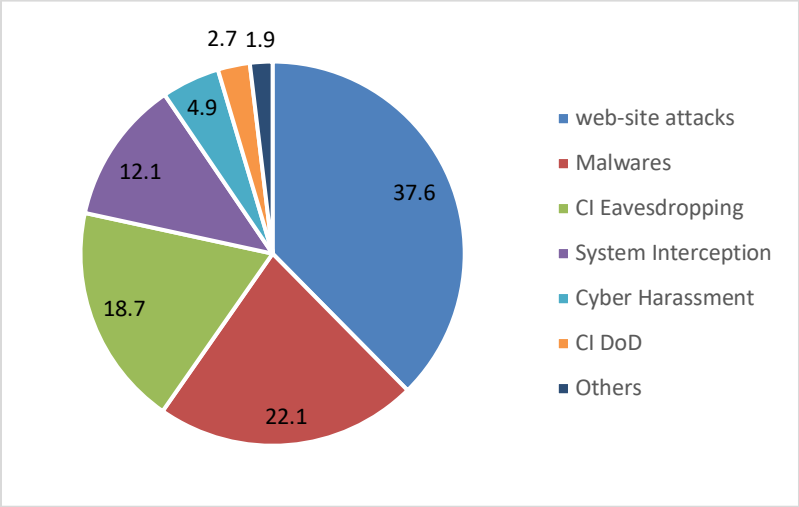

During these periods different types of cyber-attacks were targeted toward Ethiopia. For instance, the distribution of cyber-attacks that were attempted in the year 2020, including harmful malware,

[77] Interview with Seblewoyne Assefa, Head of Ethiopian Computer Emergency Readiness and Response Team, Information Network Security Agency, (Jan 5, 2021),

[78] ኢንሳይት, ኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ, ልዩ ዕትም ህዳር 2013, ገፅ 35.

website attacks, Interception, critical infrastructure eavesdropping, critical infrastructure denial of service, and cyber fraud were the most prominent ones.[79]

Figure. 2: **2020 Fiscal Year Cyber Incident Distribution Report**




### *4.2. Cybersecurity Measures in Ethiopia*

In the past two decades, Ethiopia has been exploiting the opportunity and facing the security challenges that are parallel to the ever-growing ICT infrastructure.[80] Accordingly, cyber threats and attacks are increasingly becoming an additional challenge for the socio-economic development of the country. The report of the Ethiopian Cyber Emergency Readiness and Respond Team indicates the frequency and type of cyber-attack targeting Ethiopia have increased in recent times.[81] Accordingly, this emerging cybersecurity threat across the country is attracting the attention of the government. To prevent the challenges posed by cyber threats toward the socio-economic development aspiration of the nation as well as national security, in the past decade, the Ethiopian government has taken different policy, legal and institutional measures.

#### *4.2.1. Policy Measures*

For long Ethiopia did not have a functional cyber security policy at the national that can protect its people, economy, critical infrastructure, and essential public services against cyberattacks and

[79] Information Network Security Agency, *Fiscal year report 2020/2021*, /unpublished/, 2021.
[80] Information Network Security Agency, The National Cyber Security Policy and Strategy 1 (2021)/ Draft /unpublished/.
[81] Seblewoyne, *supra* note 68.

associated risks. Even if there were different prior efforts from various actors to incorporate the issue of cybersecurity into the national agenda, it is only in 2011, that Ethiopia had its first coherent and comprehensive cybersecurity policy with the adoption of the National Information Security Policy /NISP/. The primary mission of the Information Security Policy was to create and sustain a secure, safe, and resilient information environment [cyberspace] to enable the country to use information and information infrastructure for the implementation of peace, democratization, and development programs. [82] To satisfy this mission and ensure the confidentiality, integrity, availability, and authenticity of the national information assets, the policy outlined the promotion and strengthening of international cooperation as one of its six strategic pillars. [83]

The National policy emphasizes the need to develop national cybersecurity capabilities to prevent information security threats, information warfare, and cyber terrorism through the promotion and strengthening of regional and international cooperation and coordination. The policy also reiterates the need for global collaboration on technical and legal matters to curb national, regional, and international cybercrimes, organized crimes, cyberterrorism, and other information security threats.[84] Accordingly, the policy affirms the Ethiopian government's commitment to work with nations and international organizations to ensure the integrity of the global information network through raising awareness, increasing information sharing, promoting security standards, investigating and prosecuting information security threats, and facilitating foreign investment in the sector.[85]

To resolve the jurisdictional issues emanating from the borderless nature of cybersecurity and to promote global efforts and best practices, the National Information Security Policy outlines different implementing strategies. Ensuring the harmonization of all national information security policies, laws, and regulations to international laws, standards and best practices is one of the strategies adopted by the policy to complement the national cybersecurity effort. The other strategy endorsed through the policy toward promoting international cooperation is the adoption and ratification of regional and international cooperative agreements on information security issues

[82] See *id.* at 4
[83] See *id.* at 5
[84] See *id.* at 14
[85] See *id*. at 14

based on their merits.[86] The policy also further advocates for the country to actively participate in all relevant international cybersecurity bodies, panels, forums, conferences, and multi-national agencies to promote cybersecurity.

Currently, the National Information Security Policy is being modified by INSA to make it compatible with existing international treads and to address the current complex challenges facing cyberspace.[87] Prior research conducted to assess the existing information security policy indicates the policy was not successful in achieving its intended objectives and goals due to a lack of substantive content, scientific perspective, inconsistency with other national policies, and detachment of its strategic pillars and implementation tools.[88]

### *4.2.2. Legal Measures*

In Ethiopia, the regulation of cybersecurity through legislation is a relatively recent phenomenon that came in to picture in parallel with the advancement of ICT. For a long period, there was a lack of appropriate and enforceable substantive and procedural laws that can help Ethiopia adequately deal with cybercrimes and cybersecurity challenges. The delay in the proliferation of the internet witnessed in the country has played its role in delaying legislative measures within cyberspace.[89] The first attempt to regulate cybercrime was made in 2004 with the enactment of the Criminal Code of Ethiopia. In its preamble, the criminal code asserts the failure of the 1957 Penal Code in terms of properly addressing crimes born of advances in technology, and the complexities of modern life as one of the reasons for the revision of the penal code.[90] To this end, the existing Criminal code for the first time incorporates new types of crimes including Computer crimes.

Under Section II of Crimes Against Rights in Property title, the Criminal Code regulates a handful of computer crimes. Within its provisions, the Criminal Code provides substantive provisions outlawing illegal access to a computer, computer system, and computer network; causing damage

---

[86] See *id.* at 14

[87] የኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ, የሳይበር ደህንነት ፖሊሲ እና ስትራቴጂ ማብራሪያ ሰነድ, ገፅ 7 2013, (21, 2021, 9:30 AM) https://www.insa.gov.et/documents/20124/0/National+Cyber+security+Policy%26+StrategyFDRE.docx/03b2d42e-5cb3-f29e-f8f8-fe4ad3d94586?t=1639143692057&download=true

[88] See *id.* at 7-11.

[89] Kinfe Micheal Yilma and Halefom Hailu Abraha, *The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media*, 9(1) MIZAN LAW REVIEW 108-153 (2015).

[90] The Criminal Code of the Federal Democratic Republic of Ethiopia 2004, Proclamation No.414/2004.

to computer data, and disrupting the use of a computer.[91] To this end, the Criminal Code provides different punishments for the perpetrators of these crimes ranging from simple fines up to rigorous imprisonment not exceeding five years.[92] Apart from these specific crimes the Code also criminalizes actors involved in the facilitation of the aforementioned crimes by way of importing, producing, selling, offering, distributing, buying, receiving, and possessing instruments, secret codes, and passwords with simple imprisonment and/or fines.[93]

The Ethiopian Government issued the first comprehensive cybercrime proclamation in 2016, to address, the challenge that exists in terms of regulating offenses committed within cyberspace. Research conducted before the enactment of this proclamation demonstrates the gaps that exist within Ethiopian laws in regulating the new and sophisticated types of cybercrimes as well as computer-enabled old crimes.[94] The major gap concerning the Criminal code was the absence of procedural and evidentiary provisions that are necessary to investigate and prosecute computer crimes. The Code also failed to incorporate emerging computer crimes that are affecting major corporations and citizens that came along with higher technology dependency in the country. The Computer Crime Proclamation No.958/2016 similarly cites the inadequacy of existing laws in preventing, controlling, investigating, and prosecuting suspected cybercriminals as one of the reasons for the government to enact the law.[95]To this end, the proclamation was enacted to address these challenges and combat cyber-related offenses that are a threat to the countries growing information infrastructures and digitalization initiatives.

This Computer Crime law contains substantive, procedural, and other preventive provisions that are necessary to mitigate harm targeting individuals, organizations, and public infrastructures. The substantive provisions of the Proclamation include laws that prohibit a specific type of cybercrime in three categories. The first category of cybercrimes incorporated those crimes targeting the confidentiality, availability, and integrity of computer systems and computer data. These mainly include illegal access, Illegal interception, Interference with a computer system, causing damage to computer data, and other related offenses.[96] In this regard, taking into account the rapid

[91] See *id.* at Art.706, 707, and 708.
[92] See *id*.
[93] See *id.* at Art.709.
[94] ኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ, የኮምፒውተር ወንጀል አዋጅ ማብራሪያ, 2005 ዓ.ም, ገፅ 3.
[95] Computer Crime Proclamation No.958/2016, Negarit Gazeta No. 83, 7th, July, 2016, page 9104.
[96] See *id.* at Art. 3, 4, 5, 6 and 7.

technological advancements and complexity of cyberspace, the proclamation seems to recognize the challenge of illustrating all known types of cybercrimes. Accordingly, the proclamation prefers to use technology-neutral terminology to make the law applicable to future cases. For the aforementioned crimes targeting computer and computer data, the Proclamation set different levels of criminal culpability ranging from one-year simple imprisonment up to 25 years rigorous imprisonment depending on the degree of the illicit act.[97] The criminal liability of such acts will be aggravated if such crimes are committed against legal persons, critical infrastructures, and top secrets designated for military or international relations purposes or if they are committed during a state of emergency.[98]

The second category of computer crimes stipulated under the proclamation is computer-related forgery, fraud, and theft.[99] These are crimes that exist throughout human history that are enabled and empowered by technology. The last category of crimes under the proclamation are crimes related to illegal content data like obscene or indecent crimes against minors, crimes against liberty and reputation of a person, crimes against public security, and dissemination of an advertisement.[100] The procedure part of the proclamation incorporates several provisions necessary to investigate and prosecute cybercrimes. Owing to the non-territorial and complex nature of cybercrime the proclamation also provides an international cooperation clause, stating the need to cooperate and enter into agreements with other countries' competent authorities concerning the exchange of information, joint investigation, extraditions, and other assistance. [101]

### *5. Institutional Measures*

The fight against emerging cybersecurity threats requires an effective institutional structure at the national level that can enforce national cybersecurity policies, strategies, and legislation enacted by the government. Accordingly, institutional measures include all national governance and coordination mechanism set up by the government to reliably deal with cyber threats and incidents. Despite the government initiative to embrace ICT into the country's socio-economic agenda, for long Ethiopia did not set up a national cybersecurity agency that is solely responsible for the

[97] See *id.* at Art. 7(5) and 8.
[98] See *id.* at Art. 3, 4, 5, 6 and 7.
[99] See *id.* at Art. 9, 10, and 11.
[100] See *id.* at Art. 11, 12, 13, 14 and 15.
[101] See *id.* at Art. 42.

protection of the country's growing ICT infrastructures and services. Due to this, most institutions disregard the issue of cyber security while some ICT infrastructures, internet service providers, and institutions are forced to develop their cybersecurity standards and management systems to deal with their cybersecurity challenges.[102]

Even though the former Ethiopian Information Communication Technology Authority was given the power to deter and offset national security threats emanating from ICT utilization,[103] the first attempt to establish a national cybersecurity organ was made with the establishment of the Information Network Security Agency /INSA/. Before the formation of INSA in 2006 Information Network Security Center was established under the FDRE Ministry of Defense with 37 military members.[104] In the same year, this center was upgraded to INSA with the enactment of Regulation No.130/130. INSA was established to ensure the security of the country's use of information and information communication network technologies so that they can help enforce peace, democratization, and development programs.[105]

Since then, the Agency has to be re-established twice through regulation No 250/2011 and proclamation 808/2013 to cope with the growing need of the nation and contemporary cybersecurity challenges. In addition to ensuring the security of information and information infrastructures, in the existing Re-establishment Proclamation, the Agency among other things is empowered to defend and take countermeasures against any cyberattacks targeted against the national interest and citizens' psychology.[106] Similarly, the Agency is also mandated to establish necessary international collaboration while discharging its mission.[107] This mandate was further reaffirmed with the enactment of Information Regulation No.320/2014 which provides a general guide as to the Agency International cooperation engagement by stating all interaction with foreign government

[102] Hannibal, *supra* note 73.
[103] Art.6(2) of Ethiopian Information and Communication Technology Development Authority Establishment Proclamation No. 360/2003, Federal Negarit Gazette No.82, 2nd, July 2003, page 2327.
[104] ኢንሳይት, *supra* note 69, at 20.
[105] Art. 6 of Information Network Security Agency Establishment Council of Ministers Regulation No.130/2006, Federal Negarit Gazeta, No 5, 24th, 2006, Page 3498.
[106] Art. 6(4) of Information Network Security Agency Re-establishment Proclamation No 808/2013, Federal Negarit Gazette No.6, 2nd, Jan 2012, page 7132.
[107] See *id.* Art 6(18).

institutions, security institutions, and associations to be in a manner that ensures the protection of national interest and respect the sovereignty of the country.[108]

The other institutional setup established to adequately and effectively respond to cybersecurity incidents is the National Computer Incident Response Center (CIRC). CIRC which was later renamed as Ethiopian Cyber Emergency Readiness and Response Team (Ethio-CER$^2$T), is established within the structure of INSA,[109] to serve as a single point of contact for reporting and responding to cybersecurity incidents in Ethiopia. Accordingly, Ethio-CER$^2$T assists organizations and the general public in preventing and handling cyber-security incidents collaborate with law enforcement agencies and local authorities, and coordinates national cybersecurity response.[110] Ethio-CER$^2$T Monitor the country's cyberspace 24/7 to quickly identify and respond to potential cyber incidents. Once a cyber incident is identified or reported Ethio-CER$^2$T first tries to contain the damage of the attack. Afterward, the Team proceeds to collect necessary artifacts and tries to analyze the cause and the objective of the attack. In doing so, Ethio-CER$^2$T works closely with other regional and global partners like AfricaCERT and Firs.org.[111]

### *6. International Cooperation Toward Secure Cyberspace in Ethiopia*

The non-territorial and increasingly sophisticated landscape of cyberspace and its global security threats demand cooperation and collaboration between states, international organizations, and other global actors. Cyber threats and cybercriminals cannot be bound to geographical locations and, states cannot shut down their boundaries to incoming cyberattacks.[112] Hence, there is no country in the world including Ethiopia that is capable of assuring and protecting cyberspace and its critical infrastructure from cyberattacks without having a wide range of international partners. International best practices reveal to large extent cybersecurity depends on the political will of different actors

[108] Art. 17(2) of Information Network Security Agency Re-establishment Proclamation Execution Council of Ministers Regulation No.320/2014, Federal Negarit Gazette No.78, 22nd, Oct 2014, page 7695.
[109] Information Network Security Agency Re-establishment Proclamation No 808/2013, *supra* note 106, at Art. 6(4).
[110] Seblewoyne, *supra* note 68.
[111] See *id.*
[112] ITU, ITU GLOBAL CYBERSECURITY AGENDA: FRAMEWORK FOR INTERNATIONAL COOPERATION IN CYBERSECURITY 10 (2007).

to come together and collaborate on the issue of information and intelligence sharing and mutual assistance.[113]

Accordingly, the Ethiopian government views international cooperation as a means of securing the country's information assets through the adoption of NISP and different cybersecurity legislations. Since the enactment of this policy INSA as a government agency mainly responsible for the implementation of the policy was largely engaged in harmonizing cybersecurity legislation and standards with international best practices. [114] During the drafting of the Computer Crime Proclamation No.958/2016, different efforts were made to harmonize the draft legislation with international experience and model laws aiming to create a conducive global cooperation environment for cybercriminals' exchange through the application of the double criminality principle. [115] In doing so, the drafting of the proclamation consults with various international experiences such as the European Council Cybercrime Convention, ITU model cybercrime law, UN Economic and Social Commission for Western Asia /ESCWA/ model cybercrime law, G8 cybercrime prevention principles, and UN Computer crime-related decisions as well as different African, European and American cybercrime legislations.[116]

In addition to the Computer Crime Proclamation, the 2009 Critical Mass Cybersecurity Requirement Standard /NCMCS/ enacted by INSA to secure and certify the critical information and information system of federal and regional government organizations and key private organizations of the country is also largely based on internationally accepted best practices. This national standard is well harmonized with other globally endorsed practices as well as International Organization for Standardization /ISO/ approved standards.[117] Similarly, the drafting process of the new draft National Cybersecurity Policy and Strategy indicates several attempts that have been made to harmonize the draft policy with relevant international cybersecurity best practices[118] Accordingly,

[113] UN Chronicle, Towards Cyberpeace: Managing Cyberwar Through International Cooperation, (Jan.10, 2021, 10:33 AM) https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.
[114] Hannibal, *supra* note 73.
[115] Interview with Seble Girma, Head of Legal Affaires Directorate, Information Network Security Agency (Jan 5, 2022).
[116] ኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ, *supra* note 94, at 5.
[117] INFORMATION NETWORK SECURITY AGENCY, CRITICAL MASS CYBER SECURITY REQUIREMENT STANDARD VERSION 1.0 10 (2011).
[118] Hannibal, *supra* note 73.

one can appreciate the government's commitment to keeping the promises made within the NISP in terms of harmonizing the countries policies, legislation, and standards.

On the other hand, contrary to the harmonization efforts, the government's commitment toward engaging in global cybersecurity platforms and bodies is very much limited. Apart from some endeavors made to be a member of global cybersecurity bodies such as First.org and AfricaCERT (CERT-to-CERT arrangements), Ethiopia's engagement in international cybersecurity bodies and organizations is almost nonexistent. In the current context when it comes to cybersecurity issues, Ethiopia is a passive participant in almost all international, regional and sub-regional levels as well as other less formal settings. This being the case, it is difficult to find an effort made by the government concerning signing bilateral and multilateral agreements within the context of cybersecurity. Due to this, Ethiopia is not a signatory to both the African Union Convention on Cyber Security and Personal Data Protection /Malabo Convention/and the Council of Europe Convention on Cybercrime which is open to any non-member states around the world.

Recognizing the potential benefits of being a signatory to these agreements in terms of attracting investment and strengthening Ethiopia's cybersecurity capabilities, INSA is starting efforts toward conducting a national survey to study the impact of joining the Malabo Convention.[119] However, the process is in its early stage and faces challenges in terms of bringing together different stakeholders to pursue this endeavor. Especially, considering the Convention accommodation of issues other than cybersecurity such as data security and electronic transactions and trade, other government stakeholders the likes of the Ministry of Trade and Regional Integration and the Ministry of Innovation and Technology are expected to take part in the process of adopting this regional convention.[120] However, contrary to the ongoing effort to study the impact of signing, there is no available evidence to suggest there is a plan to consider being a member of the European Council Cybercrime Convention. Similarly, there is an absence of data that can attest to the fact that Ethiopia has entered into any bilateral agreement with any other state on the issue of cybersecurity. Consequently, one can argue not being part of these two available multilateral agreements and bilateral agreements would harm the country's cybersecurity capabilities in terms

[119] See *id.*
[120] See *id.*

of accessing cybersecurity technology; cross-border criminal exchange and investigation; information and intelligence sharing; capacity building; and mutual assistance.

### *7. The Global Cybersecurity Regulation Efforts and its Relevance to Ethiopia*

Ever since Russia's made the first proposal to the General assembly in 1998, the issue of global regulation of cyberspace in the context of international security has been at the forefront of the UN agenda. Accordingly, several platforms have been formed under the umbrella of the UN for member states to discuss the topic of international law applicable to cyberspace and advancing norms governing responsible states' behavior toward cyberspace. Notably, the debate that took place among states within the framework of the GGE and the newly formed OEWG is actively shaping the global understanding of the contemporary issue of cyberspace governance. Even though these global debates are largely entangled by geopolitical differences, they have resulted in some positive progress toward advancing the global cybersecurity environment through the recognition of international law applicable in cyberspace and the adoption of 11 norms that dictate responsible state behavior in Cyberspace.

However, to date, these global debates are largely influenced by developed nations of the world while most developing nations of the world including African states remain silent or passive on the issue. As the world moves toward cyber diplomacy to ensure their national interests in these sorts of international platforms, African countries [including Ethiopia] have been largely absent from the evolving UN-based cyber norms development over the last two decades.[121] Due to the region's cybersecurity maturity level and other competing policy priorities, cybersecurity was given less priority in many African countries.[122] Since 2004, only Kenya, Egypt, South Africa, Mali, Ghana, Mauritius, Senegal, Botswana, and Morocco have held membership in the UN GGE, while Egypt, Kenya, and South Africa each took part in three of the 6 GGE groups formed by the GA. Hence, most of the outcomes of GGE platforms, including the 2015 11 voluntary UN norms are not grounded in the current realities of the resource-constrained continent with different levels of ICT development.[123]

---

[121] Directions, Partnering with Africa on Cyber Diplomacy, (Jan.11, 2021, 10:33 AM), https://directionsblog.eu/partnering-with-africa-on-cyber-diplomacy/.
[122] See *id.*
[123] See *id.*

Accordingly, like most African nations, Ethiopia has never been elected to serve as a member of the Six GGE established by the UN to advance responsible states' behavior in cyberspace between 2004 and 2019. Subsequently, when the global debate was opened to all the Member States of the UN through the introduction of the Open-Ended Working Group in 2019, the Ethiopian government failed to seize the opportunity to provide an opinion or a statement regarding the country's position concerning the ongoing global cybersecurity debate. Hence, contrary to the policy commitment made toward actively engaging in this form of the international platform in advancing the country's cybersecurity capabilities, Ethiopia is mostly absent in this UN-based norm-setting process. Interview conducted among relevant members of the government coupled with a lack of any viable evidence to that effect suggests Ethiopia has no established positions in terms of what has been discussed and debated on these international platforms.

The only available evidence suggesting Ethiopia's involvement in these global debates is the statement made at the first substantive session of the OEWG held between 12-16 December 2021. A statement made on behalf of Ethiopia concurs with the Non-Aligned Movement and does not take any side concerning the global cybersecurity regulation agenda.[124] Even if Ethiopia did not hold any concrete position toward this UN-led platform, however, the country emphasizes the advantages of rule-based order.[125] Accordingly, Ethiopia's permanent representative to the UN Ambassador Taye Atske-Selassie states *".... treaties with the strongest guarantee of reciprocity stand a better chance of compliance and uninterrupted application."*[126] In the same statement, Ambassador Taye Atske-Selassie provides an impetus for the development of an equitable international order that promotes an open, secure, stable, accessible, and peaceful ICT environment.[127] Accordingly, from a reading of this statement, one can observe Ethiopia prefers to stay neutral without establishing any position on the matter.

Despite the statement made during the first OEWG substantive session, Ethiopia's involvement in this ongoing global dialog is passive and low on the government's priority agenda. However, some efforts have been recently made by INSA to incorporate cyber diplomacy into the wider national

[124] Statement On Behalf of The Federal Democratic Republic of Ethiopia: At the First Substantive Session Of the Open-Ended Working Group on Security of And in The Use of Information and Communications Technologies 2021–2025: Delivered by Ambassador Taye Atske-Selassie, 12 – 16 December 2021, New York
[125] See *Id.*
[126] See *Id.*
[127] See *Id.*

security and foreign policy agenda through the newly drafted national cybersecurity policy.[128] Currently, INSA is also on the onset of conducting national research to identify the possible responsible stakeholders and demarcate the role they are going to play in terms of handling cyber diplomacy and taking part in the ongoing global cybersecurity agenda.[129] Even though, the approach followed to address such a sensitive and highly geo politicized issue through research is commanding, the current efforts are long overdue.

Not having a national position concerning the ongoing debate on establishing international regulation and code of conduct or norms of state behavior in cyberspace will have an impact on Ethiopia's capability to defend against cyber security threats, vulnerabilities, and attacks. Without reliable global partners and allies, the country's ability to acquire technical and financial assistance, technological transfer, information sharing, capacity building programs, and experience sharing will be affected. Besides, the lack of a rational and well-established position on the global cybersecurity debate may force Ethiopia to support other developed nations' global norm-setting initiatives without analyzing the merit of its term.

The absence of Ethiopia in this global debate and the lack of a clear position will affect the country's interest, in terms of adopting and implementing norms developed over the year to regulate cyberspace. Considering Ethiopia's limited financial resources, institutional capacity, and technological advancement, most of the current UN-based voluntary norms to govern responsible states' behavior in cyberspace are not in line with the country's cyber maturity level. For instance, norms like states' responsibility for cyberattack committed in their territory toward another state's critical infrastructure,[130] would put Ethiopia in a disadvantageous position considering the country's ability to screen, detect and guard its networks are limited. Since most of the norms adopted by the GGE in 2015 were largely influenced by developed countries, they tend to disregard the digital divide and capacity difference that exists between developed countries and developing countries like Ethiopia. Hence, the lack of necessary cybersecurity capacity will hinder Ethiopia's ability in upholding or implementing these UN-based norms.

---

128 Information Network Security Agency, *supra* note 80, at 21.
129 Hannibal, *supra* note 73.
130 U.N. GA, *supra* note 50, at 8.

Despite having a clear policy direction and legal ground to pursue Ethiopian cybersecurity interests through international cooperation and diplomacy, Ethiopia's involvement in the global cybersecurity agenda is largely hampered by various challenges. Among these challenges, the lack of awareness among relevant stakeholders as to the ongoing global debates on cybersecurity and their implication is very much observed. There is only limited knowledge within INSA cybersecurity professionals regarding the stakes and tones between the two blocks regarding the global cybersecurity regulation issues. Similarly, the lack of capable diplomats that are well acquainted with the current cybersecurity landscape and its real impact, was also observed as another challenge that adversely affected Ethiopia's bargaining power in global cybersecurity platforms. Apart from this obvious awareness and capacity gaps, weakness witnessed in terms of collaboration and alignment among different stakeholders is also a challenge to the country's international cooperative efforts. Considering cybersecurity is a cross-sectoral issue, there is an absence of structured discussion and coordination among all relevant public and private stakeholders at the national level to shape and coordinate the country's position and response to this ongoing debate[131].

The other challenge affecting Ethiopia's international cooperative endeavors lies in the fact that the issue of global cyberspace governance is intertwined with a geopolitical struggle between the major cyber powers. The competition between the US and its allies on one side and Russia, China, and their allies on the other concerning the global cybersecurity norm-setting process creates a difficult environment for developing countries. With cyberspace fast becoming a new frontline for opposing norms and influence, different countries are launching different initiatives to seek as many countries as possible in their corner. In light of these recent developments, supporting a cyber norm-setting initiative in these developed countries becomes an integral part of bilateral cybersecurity agreements. [132] Hence, entering into an international cybersecurity agreement with one of these opposing states will most likely affect Ethiopia's foreign relations with opposing states. Accordingly, considering Ethiopia's long-standing foreign policy principle which is based on neutrality and impartiality, entering open-ended /non-exclusive/ agreements and reaching consensuses with developing countries is becoming a real challenge.

[131] Hannibal, *supra* note 73.
[132] See *id.*

## 8. Conclusion

As the world continues to migrate toward digital technology in managing their day-to-day activity, attacks and threats emanating from the digitally connected world have presented a new and complex set of challenges to society. Currently, challenges resulting from a complex set of cybercrimes and behaviors are adversely impacting human rights, economy, social cohesion, and critical infrastructure. In the context of responding to this emerging global security threat in recent years, cybersecurity negotiations have come to the forefront of the international agenda. Accordingly, the international community has started to engage in dialogues to regulate the malicious behavior of state and non-state actors in cyberspace. However, despite all the ongoing dialogues and debates among various actors and stakeholders, as of yet, there is no consensus as to how the existing international law would be applicable to govern the global cybersecurity environment.

The current global effort toward developing a cybersecurity norm is largely hindered by geopolitical tensions. However, despite geopolitical differences, the GGEs established under the UN composed of both of these contrasting sides have reached some important milestones in terms of advancing responsible states' behavior toward the use of ICT. Among these milestones, the recognition of the application of existing international law (UN Charter) in cyberspace in the 2013 third GGE; and the introduction of eleven voluntary norms governing responsible state behavior in cyberspace are the most fundamental.

In light of this ongoing global cyber security governance debate, the paper uncovers only a small number of states around the world that openly declare their position concerning the debate regarding responsible states' behavior within cyberspace. As of yet, these debates are largely dominated by developed nations with high cyber maturity levels while the vast majority of developing nations including Ethiopia remain silent on the agenda. Except for the neutral statement made in the first session of OEWG, Ethiopian involvement in the current dialogue is somewhat passive. Despite the implication and the stakes of these ongoing global debates in terms of determining the country's future cybersecurity and warfare competence, Ethiopia’s involvement is very much non-existent. Considering most of the norms that have been developed under the UN GGE framework are very much aligned with the interest of developed countries with advanced cyber maturity, countries with limited cyber security capability like Ethiopia would be challenged to cope with international obligations that are put in place through this newly developed cybersecurity norms. Accordingly,

not being part of this ongoing global agenda will likely have an impact on Ethiopia's prospects in terms of attaining international technical assistance, capacity building, technology transfer, funding, and cross-border collaboration on other cybersecurity issues. Consequently, taking into account the government's recent vigorous effort toward integrating the country's critical infrastructures with ICT, disregarding these global agendas would have a detrimental impact on the country's national security in the near future.

Empirical data coming out of the government show cyberattacks targeting Ethiopian critical infrastructure are on the rise. The current growing threat landscape will have an even higher impact on the socio-economic development of the country as the country becomes more and more dependent on ICT. However, in the last decade, Ethiopia has been taking some encouraging steps toward managing these contemporary cybersecurity challenges. Even though there is still more to be done in terms of their implementation, Ethiopia is actively trying to catch up with the world through the enactment of national cybersecurity policy, legislation, and the establishment of responsible agencies.

However, contrary to the aforementioned cybersecurity measures, Ethiopia's global cooperative and cyber diplomacy engagements are very much lagging even in comparison with some other developing African nations like Kenya, Egypt, and South Africa. In addition to being absent from the current ongoing global cybersecurity norm-setting debates, Ethiopia is neither a signatory to the African Union Convention on Cyber Security and Personal Data Protection nor the Convention on Cybercrime Council of Europe which is open to all countries around the world. Similarly, it is difficult to find any bilateral cybersecurity agreement signed by Ethiopia with other countries. Although Ethiopia has a clear cybersecurity policy direction and legal frameworks supporting the country's engagement in global cooperative frameworks and agendas, the study shows that the current implementation of this policy direction and legal framework is very much limited. Hence, there is an obvious lack of strategic direction to position the country in a manner that can address the issue.

Consequently, considering international cooperation is one of the most important cybersecurity measures that can be taken to mitigate cybersecurity threats, the country's reluctance on this front would have a lasting impact on the country's effort in securing critical infrastructures and addressing cyber threats. Hence, to create resilient cyberspace that is capable of supporting the

socio-economic development ambition of the country, it is recommended for the government to begin assessing the potential impact of the ongoing global cybersecurity agenda and provide a strategic direction that can promote the version of global cybersecurity norms and agreements that can closely align with the country's national interest.

# Exploring Safeguards of Privacy Right in the Digital Age: How to Regulate Invisible Intrusion in Ethiopia?

Yisak Abraham*

## Abstract

Everyone has some aspect of their personal life that should not be exposed involuntarily. Respect for privacy enhances personhood and dignity. Despite the immense significance of privacy, the extent of interference in private life has been increasing on account of emerging sophisticated surveillance technologies. It is not uncommon to notice surveillance cameras on streets, public and private places in Addis Ababa. Most often, the public does not know who is watching and the modalities of surveillance. On top of this, the images are stored and can be used for undesired purposes thereby encroaching on privacy rights. This article examines the possible threat posed by video surveillance cameras and assesses the adequacy of the existing legal framework in Ethiopia. To do so the article applies a mixed research methodology. Video surveillance rules developed elsewhere in the globe and literature in the field are analyzed through doctrinal research methodology. Foreign codes of conduct, theories, and experiences would be a good lesson in designing the Ethiopian video surveillance code of conduct. Finally, the article recommends for the adoption of a strong regulatory framework for video surveillance that aligns with international standards and best practices.

**Keywords:** video surveillance, the right to privacy, pervasive, interference, protection, regulatory framework

## 1. Introduction

The right to privacy is one of the very crucial human needs that enhances personhood and dignity. Everyone aspires for some form of privacy. Some aspects of life should be kept private and should not be disclosed to everybody. Privacy, therefore, is an aspect of human life. However, the meaning, and nature of privacy as well as "an exact line of delineating a private and public part of our life is not easy. Simply put, as it is not easy to define the term privacy as its contours are blurry. Consequently, it is claimed that the term privacy is a "slippery concept"[1] - "a concept in disarray."[2]

*LL.B., LL.M. Public Prosecutor, Hadya Zone, S/N/N/R/S. The Authtor is grateful to Dr. Tsega Andulem for the assistance rendered to Article to be accepted for publication. The author may reached at, yisakabrahamj2551@gmail.com

[1] James Q. Whitman: *The Two Western Culture of Privacy: Dignity Versus. Liberty,* Yale L. J. Vol. 113 (2004) p. 1153-54. https://www.yalelawjournal.org/pdf/246_ftn7jo8w.pdf (accessed 7/30/2022), See also Samuel D. Warren & Louis D. Brandies, *The Right to Privacy*, Harv. L. Rev. Vol. 4 No.5 (1890), p. 193 – 220). https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (accessed 7/30/22).

[2] Finn, R.L, Wright, D., Riedewald, M. "Seven Types of Privacy." In: Gutwirtch, S., Leenes, R., de Hert, P., Poullet, Y. (eds) *European Data Protection: Coming of Age*. Springer, Dordrech. (2013) p.3 https://doi.org/10.1007/978-94-007-5170-5_1 See also R.Finn and D.Wright, "Seven types of privacy" Trilateral Research & Consulting, London Michael Friedewald, Fraunhofer ISI, Karlsruhe January (2013) p.4.

No one can exactly articulate the notion of "privacy in a way acceptable to all. Scholars "[…] have frequently lamented the great difficulty in reaching a common satisfying conception of privacy,"[3] and generations often question its boundary line. Supposedly, culture, religion, and the way of life shape facts and factors that determine the contours of privacy. Be this as it may, all communities and individuals demand some form of privacy. What really privacy is, and how can we protect one's quest for privacy? The issue is more perplexing when one's privacy is unnoticeably invaded through invisible intruders.

As it can be fairly imagined, the term privacy sprung from the word "private" and defined in terms of one's interest in keeping undisclosed and undisclosable facts private. Thus, "privacy right" is *"*the right to be let alone [or] the right of a person to be free from unwarranted publicity."[4]

Despite the absence of an exact definition of the term "privacy" and the expression "privacy right," almost all states have recognized privacy right as a protectable right. Privacy is an umbrella concept that encompasses, *inter alia*, freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches, seizure, and interrogation.[5]

Though privacy right was articulated in the modern sense in academic discourse in the late 19th century, it was as old as mankind.[6] The concept of privacy emerged from the natural need to make a distinction between oneself and the other world. In ancient times, people "had a relatively limited possibility for self-determination as their private lives were strongly influenced by the state."[7] In the medieval period, individuals existed as members of a community, and so, private life was affected by constant "monitoring" conducted by other members of the society. The appearance of real privacy relates to the transformation of those small communities into cities.[8] The need for

https://www.researchgate.net/profile/MichaelFriedewald/publication/258892458_Seven_Types_of_Privacy/links/0c9605295d271f1575000000/Seven-Types-of-Privacy.pdf (accessed 7/30/2022)

[3] *Id*.
[4] *Id*.
[5] Daniel Solove, Understanding Privacy Harvard University, press (2008) p.7
[6] Adrienn Lukács *What is Privacy? The History and Definition of Privacy* https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf (accessed 7/30/2022)
[7] *Id.*
[8] *Id.*

privacy was mentioned in primitive codes like Hammurabi, Holy books (the Holy Bible, the Qur'an,), Jewish law, and ancient communities (Greece and ancient China).[9]

During the 19$^{th}$c, the new changes in the economy and society led to the transformation of the way of life that had generated change in social integration and impacted privacy. The growth of cities and population caused physical loss of privacy as people in cities had to live in crowded vicinities.[10] Further, the proliferation of invasive newspapers and other public media generated fertile ground for gossip and photojournalism.[11] Newspapers invaded private life, by exceeding hitherto untouched spaces to satisfy a prurient taste.[12] This has ignited the quest for privacy. As a result, privacy has become more important to individuals. Then, because of interference in private and domestic circles of individuals through invasive publications, a greater call for the legal protection of private matters and privacy was sprung.[13]

The right to privacy is one of the dynamic rights that have evolved through time. Today, the right to privacy is considered one of the most important human rights deserving legal protection.[14] Its meaning and elements expand with the technological advancement. Respect for privacy frees us from the worry of being watched (panoptical phenomena) and judged by those around us and enables us to control how and when we share information and so forth.[15] Undoubtedly, privacy is essential to one's autonomy and protection of human dignity thereby serving as a foundation upon which numerous other human rights are built. It is for reason that privacy right has been recognized in social as well as legal senses.[16]

Despite the crucial quest for privacy, the emerging surveillance technology, like video surveillance technology makes us wonder about the level of protection of our right to privacy. Today, personal

---

[9] Hixson, R., *Privacy in a Public Society: Human Rights in Conflict*, Oxford University Press, New York (1987) p. 3.

[10] *Id*.

[11] Bratman, B. E. Brandeis and Warren's, "The Right to Privacy and the Birth of the Right to Privacy", Tennessee Law Review Vol. 69. (2002). p. 344.

[12] Samuel D. Warren & Louis D. Brandeis *supra* note 1.

[13] *Id.*

[14] Alexandra Rengel, *Privacy in International Law Privacy as an International Human Right and the Right to Obscurity in Cyberspace,* Groningen J. of Int'l Law, Vol 2(2) (2014) p. 34.

[15] For an overview of the different theories of privacy, see Solove, D.J. "*Conceptualizing Privacy"*, California Law Review 90 (2002) P.1087-1155; Solove, D.J: *Understanding Privacy* (Harvard University Press: Cambridge, Mass.) (2009); and Nissenbaum, H. (2010), Privacy in Context (Stanford University Press: Stanford, California).

[16] Rachel Finn and David Wright *supra* note 2.

information can be accessed, not by infringing our physical space, but through invisible hands that can unnoticeably intrude our personal vicinities and get access to our most vital secrets just by a simple click for commercial or other purposes.

The issue of invisible intrusion through video surveillance systems also concerns Ethiopians, as the country has started to use highly sophisticated video surveillance devices that are planted in public and private infrastructures. Yet, the regulatory landscape is absent or weak. More specifically, questions like how far the existing Ethiopian laws address the issue of video surveillance technology and the right to privacy need scrutiny. With a view to proactively tackle the potential threats of surveillance systems lessons can be learnt from advanced systems. This article attempts to address the compatibility of public interest through video surveillance and privacy right.

After a brief discussion on provocative issue of nature and scope of privacy right in Part I, the Second Part briefly discusses the right to privacy as stipulated in the international and regional human rights instruments. Part Three examines the implications of video surveillance on the right to privacy. The regulation of video surveillance in Ethiopia from the perspective of the right to privacy and possible lessons that can be learned from advanced systems is briefly discussed in Part Four.

## 2. The Protection of the Right to Privacy under International and National Laws

### 2.1. The Right to Privacy under International Human Rights Law

Most important international human rights instruments recognize the right to privacy as a central aspect of human dignity.[17] The right to privacy is enshrined under the UDHR[18] and other bills of rights.[19] Pursuant to Art. 17(2) of the ICCPR, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks upon his honor and reputation."[20] In General Comment No.16 the committee noted that, privacy right to be guaranteed against all unlawful and arbitrary "interferences and attacks whether they emanate from

[17] Alexandra Rangel *supra* note 14.
[18] See Article 12 UDHR. It imposes a general restriction on Article 29.
[19] ICCPR, Art. 17.
[20] *Id*; The Universal Declaration of Human Rights, Art. 12.

State authorities or from natural or legal persons."[21] The Committee also attempted to elaborate on the meaning of unlawful interference – it is invasion of privacy that is not envisaged by law.

Moreover, as stipulated in General Comment No. 16, the respect to right to privacy "requires the State to adopt legislative and other measures to give effect to the protection of this right."[22] Article 12 of the UDHR provides the same rule. This has inspired numerous constitutions to follow the same suit in recognizing the requirement to take position action that has power to enforce the right to privacy, and "limit the ability of individuals, private organizations and the state to collect information about people's personal lives, or to monitor them without their knowledge or consent ever than before."[23] Regarding the substances of domestic privacy protecting laws, the spirit of the General Comment No.16 indicates that such laws must be in conformity with the provisions, aims, and objectives of the ICCPR. This builds international compatibility, while permitting some form of flexibility in domestic implementation.[24] Moreover, General Comment No.16 provides room for the possibility of limitation on privacy right.[25] As all rights are not absolute, the right to privacy also suffers from exceptional limitations. Exceptional situations cannot be presumed. There shall be an express declaration that restricts the right to privacy. The law requires the limitation should be necessary and proportional to the situation that necessities encroachment on privacy right.

## 2.2.The Right to Privacy under Regional Human Rights Treaties

### *2.2.1. Protection of the Right to Privacy in Europe*

Comparatively speaking, Europe has more developed jurisprudence on the privacy right. In Europe there are various treaties that = protect privacy. Some of them are solely concerned with the issues of privacy. Other regions have no such comprehensive normative framework that is typically meant to regulate privacy. Among the other instruments, the very important treaty in the region is the European Convention on Human Rights. Article 8 of the Convention provides:

[21] General comment No. 16: Article 17 (Right to privacy) Thirty-second session (1988), pp.1.
[22] ICCPR General Comment No. 16: Article 17 (Right to Privacy) Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988.
[23] Alexandra Rangel *supra* note 14.
[24] The UN Conference on Trade and Development, Data Protection Regulations and International Data Flows, in New York and Geneva (2016).
[25] GA Report of the Human Rights Committee (43rd session) A/43/40, (1988), par.7-9.

1. Everyone has the right to respect for his private and family life, his homes, and his correspondence.
2. There shall be no interference by a public authority with the exercise of his right except such 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. [26]

This article provides for protection against unlawful and arbitrary interferences with the right to privacy; contents of the right; obligation of member states to promulgate privacy protecting laws; and principles that governs measures limiting the right to privacy.

Next to the Convention, the most significant comprehensive privacy protection legislation having significance, not only in the region, but also in the wider world is the European community's Directive of 1995.[27] It sets standards of privacy protection to be incorporated by all members of the community in their national legal documents.[28] The directive requires that personal data be "processed fairly and lawfully; limits purpose for which personal data may be used to situations where the individual has given consent or where use is required by law; seeks to ensure the openness of data systems for scrutiny and change by data subjects; requires confidentiality and security in processing of data; and calls all member states to create an independent "supervisory authority" to monitor the application of the directive."[29] The need for supervisory organ is particularly special one in this directive than other international and regional laws.

Another very important treaty in the region is the convention for the protection of automatic processing of personal data called the "Council of European Convention on Data Protection (ETS No.108/1985)." Article 1 of the Convention stipulates:

> The purpose of this Convention is to secure in the territory of each party for every individual whatever his nationality or residence, respect for his rights and

[26] Council of Europe, European Convention on Human Rights, (4 Nov.1950) Article 8 (1 & 2).
[27] James B. Rule, *Privacy in Peril* (Oxford University press, 2007), p.31.
[28] *Id*.
[29] *Id*.

fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data (data protection).[30]

As the protection of personal data falls within the realm of private life, the convention purports to protect individuals against abuses while collecting and processing "personal data and seeks to regulate at the same time the trans-frontier flow of personal data."[31] ETS also enshrined the subjects of surveillance's rights to know what information is stored on him or her and, to have it corrected if required.[32]

The additional protocol of ETS, 1985 also enhances the protection of personal data and privacy by improving the original convention of 1981 by providing for the setting up of a national supervisory body responsible for ensuring compliance with laws adopted in conformity of the convention concerning personal data protection.[33] One more improvement is on transboundary data flow to the non-member states. Accordingly, data may only be transferred if the recipient State or IO is able to afford an adequate level of protection.[34]

#### *2.2.2. Protection of the Right to Privacy in Africa*

The African Charter on Human and People's Rights of 1981 does not expressly provide for the right to privacy.[35] But, it does not mean that there is no legal protection for privacy in the region. For instance, one can see the Declaration of African Commission on Human and Peoples Rights' (hear after, DACHPR) that shows the jurisprudence of the commission on privacy. The ACHPR expands States obligation concerning access to information and developed the standards related to new areas of concerns including a legal framework on privacy and the protection of personal information under its new Declaration on Principles of Freedom of Expression and Access to

---

30 ETS No.108/1985, Art. 1.

31 European Commission for Democracy through Law: "Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights," adopted by the Venice Commission at its 70th Plenary Session (Venice, 16-17 March 2007) Study No. 404 / 2006\p.9 &10.

32 *Id*.

33 Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Trans Border Data Flows, into force on 1 July 2004.

34 *Id*.

35 Lee A. Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties,* Int'l J. of L. & Tech, Vol. 6 (1998) p. 247 – 287). https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf ( accessed 7/30/2022).

Information in Africa (2019) or the Declaration of article 9 (the right to receive information and free expression) of the African Charter on Human and Peoples' Rights (the Declaration).[36] As per the principles 40 & 41 of the declaration, the commission directly addressed the protection of personal information and communications surveillance in the context of the right to privacy. If we see principle 42 of the Declaration, it establishes a regulatory framework for the protection of personal information that requires States to adopt laws regulating the processing of personal information.[37]

In addition, States must ensure that individuals consent to the processing of their personal information; the processing also should be "in accordance the purpose for which it was collected"[38] and not excessive; the data is deleted when the processing is complete; the processing should be transparent; and also the information should be held confidential and be "secure at all times".[39] Moreover, the principle also provided for the mandatory accessibility of personal information to the data subjects and an opportunity to object the processing. An individual also must be notified when an unauthorized person has accessed their information and must have access to "legal recourses to effective remedies in relation to the violation of their privacy".[40]

Another very important regional legal framework relevant to the right to privacy is the Malabo Convention on Cyber Security and Personal Data Protection adopted in 2014.[41] The Convention stipulates the basic principles governing the processing of personal data aiming at protecting the right to privacy. Article 13 of the Convention provides for the principles of consent and legitimacy of personal data processing; purpose, relevance and storage of processed data; accuracy of personal data; transparency of personal data processing and confidentiality and security of personal data.[42]

---

[36] Privacy International at the Sixty Second Session of the African Commission on Human and People's Rights (April 2018). https://privacyinternational.org/news-analysis/2227/privacy-international-62nd-session-african-commission-human-and-peoples-rights (accessed 7/30/2022).

[37] ACHPR, Declaration of Principles of Freedom of Expression and Access to Information in Africa 2019, principle 40-41.

[38] Principle 42.

[39] *Id*.

[40] *Id*.

[41] African Union Convention on Cyber Security and Personal Data Protection, adopted June 27, 2014, last signature May 11, 2020, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 7/30/2022).

[42] *Id*. Art. 13.

Furthermore, the convention stipulates special rules for the processing of sensitive data under article 14.[43] Accordingly, the State shall:

> " […] undertake to prohibit any data collection and processing revealing racial, ethnic, and regional origin, parental filiations, political opinions, religious or philosophical beliefs, trade unions membership, sex life and genetic information or more generally on the state of health of the data subject."[44]

Another very crucial protection is the provision for the "Data Subjects right"-the right to information,[45] to access,[46] to object,[47] and right of rectification or erasure.[48] To ensure better protection of the right, the convention also imposes obligation on the state parties to establish an independent authority in charge of protecting personal data.[49] "Preliminary personal data processing formalities" are there to be checked out by the authority concerned.[50] The treaty also imposes obligations of confidentiality,[51] security,[52] storage,[53] and sustainability[54] on the personal data controllers. At sub-regional level, the existing privacy laws framework in Africa includes the SADC Model Law on Data Protection (2010), ECOWAS Supplementary Act on Personal Data Protection (2010), and EAC Framework for Cyber Laws (2008).[55]

At a national or domestic level, many African countries have been attempting to take steps toward protecting the right to privacy, both online and offline as well. Primarily, almost all States in Africa are parties to the major international human rights instruments incorporating provisions for the protection of the right to privacy.

---

[43] *Id*. Art. 14.
[44] *Id.*
[45] *Id*. Art. 16.
[46] *Id*. Art.17.
[47] *Id*. Art. 18.
[48] *Id*. Art. 19.
[49] *Id*. Sub-art. (1),(a) of Art. 11.
[50] *Id*. Art. 10.
[51] *Id*. Art. 20.
[52] *Id*. Art. 21.
[53] *Id*. Art. 22.
[54] *Id.* Art. 23.
[55] Verengai Mabika (Senior Policy Advisor – Africa) Privacy & Personal Data Protection Guidelines for Africa p. 6 https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session%207_Verengai%20Mabika.pdf (accessed 7/30/22).

Another indication is that, nearly all countries in Africa have recognized a specific right to privacy in their constitution, and some states even have introduced somehow comprehensive privacy laws, particularly of data protection legislation.[56] Until 2016, 17 countries in Africa have enacted a comprehensive personal data protection legislation, namely Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia, and Western Sahara.[57]

As some scholars argue, the driving factor for such progress in the protection of privacy in Africa is the need for adequate protection of personal data for the trans-border flow of personal data from Europe to other States as stipulated under article 25(1) of the European Union's Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data 95/46/EC. Accordingly, the Africa's trade with Europe has posed pressure on states to ensure that their data protection laws and directives are in line with this requirement to conduct business with European countries, i.e., the economic importance of meeting the requirement.[58] Other factors are "the development of internet, the operations of multinational corporations, and the trans-national flow of data."[59]

### 2.3. The Right to Privacy under Ethiopian Laws

In Ethiopia, there is no comprehensive privacy law till now. Despite the lack of comprehensive privacy law, Ethiopia is one of the countries that expressly recognized the right to privacy in various legislation including the Constitution. Primarily, the FDRE Constitution protects the right to privacy in two significant dimensions. First, it expressly recognizes the right to privacy and stipulates the restrictive conditions/principles (necessity, legality, and proportionality) of privacy as follows:

> 1. Everyone has the right to privacy. This right shall include the right not to be subjected to searches of his home, person or property, or the seizure of any property under his personal possession.

---

[56] Arthur Gwagwa *et al*, *Protection of the right to privacy in Africa in the digital age IDRC& CRDI* (May 2014) p.7, https://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf (accessed 7/30/22).

[57] Cynthia Rich "Privacy Laws in Africa and Near East "Bloomberg BNA World Data Protection Report, 1, (2016), https://paperzz.com/doc/7620737/privacy-laws-in-africa-and-the-near-east (accessed 7/30/22).

[58] Arthur Gwagwa *et al* *supra* note 56 p.5.

[59] *Id*.

> 2. Everyone has the right to the inviolability of his notes and correspondence including postal letters, and communications made by means of telephone, telecommunications and electronic devices.
> 3. Public officials shall respect and protect these rights. No restrictions may be placed on the enjoyment of such rights except in compelling circumstances and in accordance with specific laws whose purposes shall be the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others."[60]

Sub-art. 1 encompasses possible contents of the right to privacy. But, when compare it with the contents of article 17 (1) of the ICCPR does not hold all aspects of the right to privacy.

Secondly, the constitution integrated the International Human Rights Instruments into laws of the land (Art. 9(4). Thus, the rules and principles regulating the right to privacy under the UDHR, ICCPR, CRC, Convention on the Protection of Migrants, the African Charter on Rights and Welfare of the Child (1990) and the UNGA (2013) Resolution on the Right to Privacy in a Digital Age are applicable as part and parcel of the Ethiopian privacy laws. Furthermore, the fundamental rights and freedoms including the right to privacy specified in Chapter three of the Constitution "shall be interpreted in a manner conforming to the principles of the Universal Declaration of Human Rights, International Covenants on Human Rights and International instruments adopted by Ethiopia."[61]

Though not comprehensive enough, the subsidiary laws which have extended guarantees to privacy include: article 32 &33 of the Criminal Procedure Code of Ethiopia,[62] article 6-9 & 12 of the Freedom of Mass Media and Access to Information Proclamation, [63]article 4&29(2) of the Electronic Signature Proclamation,[64] article 39 of the Income Tax Proclamation,[65] article 64(1) of the Registration of Vital Events and National Identification Cards Proclamations,[66] article 21 of the Documents Authentication and Registration Proclamation,[67] article 11, 13, 20,24, & 31 of the

---

[60] The FDRE Constitution, Proc. No. 1, 1995, Fed. *Neg. Gaz.* Year 1, No. 1, (Aug 1995) A.A., Art. 26.
[61] *Id*. 13(2).
[62] Ethiopian Criminal Procedure Code, Proc. No. 185/1961, Arts. 32&33
[63] Freedom of Mass Media and Access to Information Proclamation, Proc. No.590/2008, Arts. 12 & 6-19.
[64] Electronic Signature Proclamation, Proc. No.1072/2018, Arts. 4 & 29 (2).
[65] Income Tax Proclamation, Proc. No.286/2002, Art. 39.
[66] Registration of Vital Events and National Identification Cards Proclamation, Proc. No.760/2012, Art. 64 (1).
[67] Authentication and Registration of Documents, Proc. No. 922, 2015, Art. 21.

Civil Code of Ethiopia[68]. In the context of the specific sectors governed by these laws, the provisions impose some obligations on data collectors like, an obligation to hold personal information confidentially, and grant some rights to data subjects, for example, the right to be consulted for their consent in case their personal information required to be disclosed.

Unlawful and arbitrary interferences into the right to privacy are punishable under the Ethiopian criminal law regime. In accordance with article 604 of the Criminal Code of the Federal Democratic Republic of (hereafter the Criminal Code) "Violation of Privacy of Domicile or Restricted Areas" i.e. Entering into domiciles, or restricted areas unlawfully, and without the permission or wishes of the lawful occupant, and even refusing to leave such premises after having entered with permission or without opposition of the lawful occupant is punishable with simple imprisonment not exceeding 3 years, or fine.[69] In case of the violation "committed by a public servant who is not authorized to take such action, or who does so in violation of legal safeguards and formalities, the special provision (Art. 422) shall apply."[70] Aggravating circumstances to this offence are also listed under article 605 of the Code. Accordingly, if the offence is committed by "carrying weapons, making use of threats or resorting to violence; by a group of persons acting in common; or between the hours of 6 PM and 6 AM; or by a person holding himself on to be a public servant or official, unless otherwise authorized by law, is punishment shall by rigorous imprisonment not exceeding five years."[71]

Article 339 of the Code also stipulates breaches of professional secrecy as a crime. The Code also protects privacy of communications under article 606. Violation of the Privacy of Correspondence or Consignments is "punishable up on compliant, with a fine not exceeding one thousand Birr, or according to the circumstances of the case, with simple imprisonment not exceeding three months."[72] More severely, intentional and unlawful interceptions, destructions, retentions, or diversions from their true destination of the "correspondences or packages, is punishable upon accusation with simple imprisonment not exceeding six months, where his act does not constitute a specific crime punishable more severely."[73] However, the Criminal Code does not incorporate

[68] Civil Code of Ethiopia, Proc. No.165/1960, Arts. 11, 13, 20, 24, & 31.
[69] Criminal Code of the Federal Democratic Republic of Ethiopia, Proc. No. 414/2004, Art. 604(1).
[70] *Id* sub-art. 2.
[71] *Id.* Art. 605.
[72] *Id*. Art. 606.
[73] *Id* sub-art. 2.

all possible violations of types of privacy noted at the beginning of the article and the punishments provides for are somehow simple and it would be great if the crimes were made punishable up on accusation than upon a complaint.

Another criminal law safeguards for the right to privacy in Ethiopia are stipulated through sector-specific privacy protecting laws such as the finance sector privacy rules (the National Payment System Proclamation No. 718/2011,[74] the Payment Instrument Issuers Directive[75] and the Banking Business Proclamation,[76] ICT sector (Part II of the Computer Crime Proclamation),[77] and so on. Yet, it is possible to argue they if we examine the criminal law, we cannot get any provision that deals with the infringement of privacy through secret video cameras which are very pervasive by their nature and becoming common in Ethiopia.

Concerning judicial precedent, we have very few cases that are reported in the area of privacy. One notable case is *Riyan Miftah* v. *Elsewdi Kebels Plc*[78] in which Court ruled that images of a person cannot be publicized without consent of the person concerned. The Draft Data Protection Proclamation which is initiated by the Ministry of Innovation And Technology is expected to fill the existing gaps in the field and be used as a starting point to have a comprehensive and sufficient privacy law in Ethiopia. As to the Director General of the Legal Service Directorate in the Ethiopian Innovation and Technology Minister, the Draft Proclamation is assumed to regulate issues related to privacy comprehensively and adequately, particularly aimed to protect and minimize the technological threats posed on the right to privacy and the draft introduces an authority namely, Privacy or Data Protection Commission.[79] Currently, the draft is completed at the Ministry level and is to be sent to the Federal Attorney General soon. Also, some minimal provisions of the 2016 Computer Crimes Proclamation are expected to fill the existing gaps on the field and be used as a basement.

Despite the efforts which have been made to protect the right to privacy throughout its legal history, an adequate protection of privacy is yet to be realized in Ethiopia. As some studies

[74] National Payment System Proclamation Proc. No. 718/2011, Art. 35 (2) (e).
[75] Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020, Art 17
[76] Banking Business Proclamation, Proc. No. 592/2008, Art. 58 (7).
[77] Computer Crime Proclamation, Proc. No. 958/2016, Art. 3 – 8.
[78] Cassation Court of the Supreme Court of Federal Democratic Republic of Ethiopia, File No. 91710.
[79] Interview with Ato Hayalneh Lemma, the Legal Service Directorate Director at Ethiopian Innovation and Technology Minster, 20 April 2021.

indicated, like most African countries, Ethiopia faces contemporary challenges that threaten data protection and privacy.[80] Over the past decade, the Ethiopian government has procured and deployed numerous surveillance and intrusive technologies in Ethiopia.[81] As Berhan Taye and Roman Teshome explained in their study "Privacy and Personal Data Protection in Ethiopia", the causes for the mass violation of the right to privacy by public and private bodies in Ethiopia include, but are not limited to lack of comprehensive institutional framework, lack of implementing policy guidelines for privacy-protecting laws, absence of sufficient transparency and consultation while drafting laws, an inadequate legal framework for privacy, and the emerging pervasive technologies.[82]

## 3. The Right to Privacy in the Era of Technology: How Can We Control Invisible Intruders?

### 3.1. The Effort to Regulate Video Surveillance

Historically, the debate on the relationship between new technologies, and issues of human rights appeared in 1968 during the International Conference on Human Rights in Tehran, which brought some recommendations for deliberation by the United Nations General Assembly, hereafter (UNGA), and then the Resolution number 2450(XXIII) which mainly reflects on the protection of human right in the age of digitalization was adopted.[83]

In the world we are living today, there is a high tendency to use the emerging highly sophisticated surveillance technologies to ensure security and safety at government, business organizations and individual levels. Even some scholars argue that the protection and conceptualization of privacy cannot be detached from technological development.[84] There are a range of newly emerging sophisticated surveillance technologies such as growing automated surveillance in public places, internet surveillance, deep packet inspection, automatic license plate recognition systems, satellite monitoring, cell-phone tracking, facial recognition, CCTV, drone-based surveillance, and so forth,

---

[80] Berhan Taye & Roman Teshome *Privacy and Personal Data Protection in Ethiopia* (2018), https://cipesa.org/?wpfb_dl=379 ( accessed 7/30/2022).

[81] *Id* p.5.

[82] *Id* p.25.

[83] Coccoli, J., "The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era," *Peace, Human Rights Governance,* Vol.1 (2), (2017) p. 3&4.

[84] Ann Cavoukian, *Surveillance, then and now: Securing Privacy in Public Spaces,* (June 2013), https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-surveillance.pdf (accessed 7/30/2022).

to which the international and domestic laws have yet to respond effectively.[85] In the words of Alexandra Rangel:

> To determine the effect of new technologies on the right to privacy, and provide adequate solutions, a contextual analysis of the potential infringements that technology facilitates and the resources available for protection is essential.[86]

Unlike some other rights, the negative impact of technological advancements on the right to privacy seems to outweigh its benefits. In her study entitled "the impact of technology on the privacy of the individual," Rosenberg, concluded that; "technology continues to be viewed as a threat to privacy than a possible solution."[87] In reviewing the concept of privacy, new technologies often make us wonder what level of protection of privacy is possible in a world where personal information about us can be accessed not by interfering physical space, but by pressing a button and looking at a screen.[88] In addition, due to the development of science and technologies, the intrusion into someone's privacy is getting increased.[89] It is now very easy for companies and governments to monitor every conversation we conduct, every location we visit, and each commercial transaction we undertake. Such capabilities may lead to negative effects on individuals. They also affect how we think about the relationships between individuals, markets, society, and the state. Electronic surveillance can lead to a feeling of fear and of always being watched. Such negative impacts in turn result in loss of dignity.[90] Further, the most visible challenge to privacy is that the right can be compromised without the individual being aware of it.[91] In physical invasion of the right of privacy individuals are aware of the intrusion-being detained, censored, or restrained.[92] Besides, individuals are aware of the transgressor in case of other rights.[93] This has a great contribution in holding the transgressors responsible for what they have done, in case of unlawful and arbitrary interference. But this is very difficult in the case of

---

85 *Id*.
86 Alexandra Rangel *supra* note 14 p. 10.
87 Rosenberg, The Impact of Technology on the Privacy of Individual, (1994), http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html (accessed 7/30/22).
88 Alexandra Rangel *supra* note 14 p. 1.
89 Adrienn Lukács *supra* note 6.
90 J.J.Britz, *Technology as a threat to privacy: ethical challenges to the information profession* university of Pretoria South Africa, http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html, (Accessed 7/30/22).
91 Privacy International, https://privacyinternational.org/explainer/56/what-privacy (Accessed 7/30/22).
92 *Id*.
93 *Id*.

the right to privacy as the interferer's hands are most of the time invisible. We are also not being informed about the monitoring we are placed under and are not equipped with the capabilities or given the opportunity to question those activities. That means the surveillance technologies are excluding us from being involved in decisions about how our lives are interfered with, our information processing, our bodies securitized, and our possessions searched. So, secret surveillance is posing a great danger, because of its intrusiveness, lack of accountability and so on.[94]

While Government organs use technologies for the sake of law enforcement,[95] Even "surveillance of specific individuals- often journalists, opposition figures, critics and others exercising their right to freedom of expression has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings."[96]

One of the threats to privacy rights is the collection of a large amount of personal data by government organs, without adequate legal, regulatory, and policy frameworks.[97] Usually, most of African countries, including Ethiopia face such challenges too.[98] For example, over the past decade, the Ethiopian government has procured and deployed numerous surveillance and intrusive technologies.[99]

### 3.2.The Threats of Video Surveillance on the Right to Privacy

Despite the significant benefits brought by technological advancements all over the world, surveillance technologies, including video surveillance, pose direct and indirect human rights infringements. This Section focuses on video surveillance technology and its possible threat to privacy. As a mechanism of tackling terrorism, the widespread use of surveillance technology has become a common phenomenon even in Ethiopia. Basically, "surveillance camera system" is a system that includes the Closed Circuit Television (herein after CCTV), Body Worn Video, Drones, Dashboard Cameras, Automatic Number Plate Recognition (ANPR), Automatic Facial

---

[94] *Id.*
[95] Ann Cavoukian, *supra* note 84.
[96] UNHRC, Special rapporteur, surveillance and human rights, human rights council –forty –first sessions, https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session41/list-reports (Accessed 7/30/22).
[97] Berhan Taye & Roman Teshome *supra* note 80.
[97] *Id.* p.2.
[98] *Id.*
[99] *Id.* p.5

Recognition (AFR) technology etc.[100] CCTV is a system that allows one to keep an eye on what is going on in and around certain premises.[101] Cameras and monitors enable us to view events live and recorded footage for later reference**.** CCTV, therefore, is an electronic surveillance tool that employs a "network of cameras to monitor a particular area for protection against violence, terrorism, theft,"[102] vandalism and other criminal acts as well.

The sophisticated video surveillance system may include *thousands of cameras linked together* making use of technology to automatically identify and track a particular person from one location to another.[103] The cameras are enabled to pan, tilt, diagnose and provide a lot more detailed images of even very distant objects than previously possible. There is a camera that has 60 times optical zoom lens that can read even tiny letters like terms written on a cigarette pack at 100 yards.[104] More surprisingly, even 400 times magnification cameras have been deployed in some cities.[105]

Also, improved quality of recordings, reduced storage costs, and the use of digital technology enabled traversing and exploitation of recorded data in ways previously impossible with analogue recording systems. Furthermore, although facial recognition and other biometric systems are yet in their infancy, advancements in these areas can be integrated with CCTV systems to track movement in their field of view or across networked cameras allowing an operator to automatically follow a target object in an entire city in real-time or the stored data.[106] As a result of improvements in video surveillance technology, the system is cost-effective and efficient to fight severe threats to public safety with minimum human power. Due to this advantage of CCTV, nowadays, there is high interest to use the technology. For instance, there are more than 4 million cameras in the

---

[100] See the United Kingdom Protection of Freedom Act of 2012 (PoFA), Section 29(6).

[101] See State systems, https://www.statesystemsinc.com/blog/what-is-cctv (Accessed 7/30/22).

[102] Mahmoud Rajpoot, Q., & Jensen, C. D, "Video Surveillance: Privacy Issues and Legal Compliance," In V.Kumar, & J. Svensson (Eds.), Promoting Social Change and Democracy through Information Technology IGI global, (2015). https://backend.orbit.dtu.dk/ws/files/110934780/Video_Surveillance_Privacy_issues_and_legal_compliance.pdf (Accessed 7/30/22).

[103] Moncrieff, S., Venkatesh, S., & West, G. A. *Dynamic Privacy in Public Surveillance* (2009) p., 22–28.

[104] Slobogin, C. Camera *Surveillance of Public Places and the Right to Anonymity*, Mississippi Law Journal, 72(1), (2002) p. 213−233.

[105] Stephen Kinzer, *Chicago Moving to Smart' Surveillance Cameras*, The New York Times, https://www.nytimes.com/2004/09/21/us/chicago-moving-to-smart-surveillance-cameras.html, (Accessed 7/30/2022).

[106] *Id*.

UK alone, [107] and it is estimated that an average person in London is caught on camera around 300 times a day.[108]

The use of the surveillances system is backed by a legitimate purpose. Its primary aim was to tackle people and transactions that are potentially dangerous for the maintenance of peace and security. Continuous surveillance is assumed to reduce destructive crimes ranging from terrorism to traffic regulation. However, the practice does not guarantee the system would work. In the UK, where surveillance cameras (more than 4 million) have been extensively deployed in public places, crime rates never changed.[109]

Ruther, the combination of the pervasive form of the system with the technological advancements such as high resolution, magnification, identification, and tracking have the potential to disrupt the balance between the need for managing peace and security, and the right to privacy. It is reported thatthe right to privacy is at stake because of extensive video surveillance. For example, in a report by the BBC in 2005 two Council CCTV workers used the technology CCTV cameras to spy a naked woman in her home.[110] In another incident reported by the Guardian in 2010, an airport worker at Heathrow Airport was given a police warning for harassing a female after he allegedly took a photo of a female colleague as she went through a full body scanner at the airport.[111] Studies undertaken on how the CCTV systems in Britain are operated have also found that most of the time, male operators usually use the system to voyeuristically spy on women.[112] The researchers found that one in 10 (ten) women was targeted for entirely voyeuristic reasons in the UK.[113]

---

[107] Norris, C., McCahill, M., & Wood, D. *The Growth of CCTV: A Global Perspective on the International diffusion of video surveillance in publicly accessible space. Surveillance and Society*, (2004) 2(2), 110–135. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3369/3332 (Accessed 7/30/2022).

[108] Reported by BBC news 2002. CCTV: Does it work? Retrieved 4, 8, 2022, from: http://news.bbc.co.uk/1/hi/uk/2071496.stm.

[109] American Civil Liberties Union "what is wrong with public video surveillance" (2021), Available on:https://www.aclu.org/other/whats-wrong-public-video-surveillance.

[110] BBC News, *CCTV staff spied on naked woman* (2005), Retrieved from http://news.bbc.co.uk/2/hi/uk_news/england/merseyside/4503244.stm (accessed 7/30/2022).

[111] The Guardian, Airport *Worker Given Police Warning for Misusing Body Scanner* https://www.theguardian.com/uk/2010/mar/24/airport-worker-warned-body-scanner (Accessed 7/30/2022).

[112] American Civil Liberties *Union What is Wrong with Public Video Surveillance?* (2021), https://www.aclu.org/other/whats-wrong-public-video-surveillance (Accessed 7/30/2022)

[113] American Civil Liberties Union 2022, https://www.aclu.org › other › testimony-aclus-barry-steinhardt-surveillance-system-dc-city-council. (Accessed 7/30/2022).

Another important incident that was reported in the United States revealed that the New York City police in a helicopter while monitoring the crowds at the "2004 Republican Convention trained an infrared video camera on an amorous couple enjoying the night time "privacy" of their rooftop balcony."[114]

The other problem involving video surveillance systems is the unauthorized collection and processing of data. This may result in unlawful interception of data, "especially, if the data have been collected by covert surveillance methods."[115] Special problems happen when data collected by such means are used for purposes other than motives other than public objectives. The ECHR's jurisprudence in the *Peck vs. UK* [116]provides a vivid rule in video surveillance. The facts of the case were:

> The applicant was captured on CCTV as he carried a large knife and was in the process of attempting suicide. The police were able to prevent him from causing himself fatal harm. The CCTV footage was subsequently released to the press in order to demonstrate the effectiveness of CCTV.[117]

The ECHR decided that the disclosure of the CCTV footage exceeded security observation and surpassed a degree that the applicant could have possibly imagined. "The disclosure by the Council of the relevant footage, therefore, constituted a serious interference with the applicant's right to respect for his private life."[118]

Another impact of video surveillance on the right to privacy is its "chilling effect on public life"[119] or panoptical effect. The idea is that, when people are aware of being observed or might be observed at any moment by surveillance cameras, compelled to change their behavior in public

---

[114] American Civil Liberties Union "what is wrong with public video surveillance" (2021), Available on:https://www.aclu.org/other/whats-wrong-public-video-surveillance (Accessed 7/30/2022).

[115] European Commission for Democracy through Law: "opinion on video surveillance in public places by public authorities and the protection of human rights" Adopted by the Venice Commission at its 70th Plenary Session (Venice, 16-17 March 2007) Study No. 404 / 2006, pp.

[116] 36 EHRR 41 (2003). https://www.google.com/search?client=safari&rls=en&q=36+EHRR+41+(2003)&ie=UTF-8&oe=UTF-8 (Accessed 7/30/22).

[117] *'Peck v UK, Id*

[118] European Commission for Democracy through Law: "opinion on video surveillance in public places by public authorities and the protection of human rights" Adopted by the Venice Commission at its 70th Plenary Session (Venice, 16-17 March 2007) Study No. 404 / 2006.

[119] American Civil Liberties Union, "what's wrong with public video surveillance?" available on: https://www.aclu.org/other/whats-wrong-public-video-surveillance (2021).

places. One columnist expressed, "if we know that we are being monitored by armed government agents we tend to put a damper on things. Also, we don't want to offend them or otherwise call attention to ourselves."[120]

The widespread use and massive deployment of CCTV, therefore, is a great concern for public and seen as a threat to privacy by critics and so forth. Thus, taking into consideration the immense impact of video surveillance on the right to privacy, this is the right time to regulate the use of surveillance cameras while the system is in its infancy.

## 4. Video Surveillance and Privacy Rights in Ethiopia

### 4.1. The Current Practice and Potential Growth of Video Surveillance in Ethiopia

The cheap availability of CCTV surveillance systems[121] and the threat posed by terrorism and other security issues caused Ethiopian security forces to rely on video surveillance systems in the streets of Addis Ababa, government offices, and other public places. Currently, it is not unusual to notice security cameras installed in Bole Street, Meskel Square, hotels, malls, industrial parks, airports, offices, and even individual residential areas.

Despite the wide availability of video cameras in Ethiopia, the use of sophisticated video surveillance technology is still in its infancy, but the high interest is apparent. An Ethiopian Video Surveillance System Market report, conducted by 6Weresearch in Sep 2019 suggests that the "growing construction projects in the industrial, manufacturing, and power utility sector owing to the surge in foreign investments in the country would drive the market for video surveillance system in Ethiopia."[122] Above all, the requirement " […] for the compulsory installation of surveillance camera in public would result in a further surge in deployment of surveillance cameras in the country."[123] It is further suggested that due to increased investments in security solutions in the newly constructed manufacturing and industrial sector in the country. the Ethiopia video surveillance system market size is expected to grow during 2019-2025. Addis Ababa is a key city

[120] *Id.*
[121] The CCTV cameras are available at price starting 4000-300,000 Birr in Ethiopia ( Interview with Bereket Abraha (Engineer), the Network Administrator in ECO-Engineering Plc. April 22 2021).
[122] 6Wresearch, "Ethiopia Video Surveillance System Market (2019-2025)-size, share, and trends" Available: on http/www.com6Wresearch.com/industry, (Sept. 2019).
[123] *Id.*

in Ethiopia registering maximum installation of surveillance cameras. The construction of unforeseen types of high rise buildings in financial districts including state of the art building of the Commercial Bank of Ethiopia and Maritime Transit Shipping Enterprises Headquarters, Nib Bank, Hibret Bank and so forth, supposedly planted with cameras with multiple zooming capacities.[124]Apart from this, there exists more than 115 CCTV distributors found in Addis Ababa even at this stage.[125] This also proves the potential for the faster and wider spread of the system in Ethiopia.

Now considering the ongoing reality and interest in digital surveillance in Ethiopia, it is a practical necessity to examine the power of the Ethiopian regulatory and institutional framework that is meant to address the impending issues that may possibly arise from the use of video surveillance technology and the right to privacy. As noted elsewhere above, while there are several privacy laws governing specific sectors and aspects, there is virtually no legislation that directly deals with the use of video surveillance in the context of the right to privacy. Therefore, even though the existing sector-specific privacy rules provide a limited protection against unlawful and arbitrary interference to the right to privacy, there are currently no general legally enforceable rules to limit privacy invasions through the CCTV and protect against the abuse of the system in Ethiopia. There is also no evidence whether each sector (public or private) has its own laws or practices for video surveillance in Ethiopia. The upcoming Draft Data Protection Proclamation also does not specifically address the issues of video surveillance in the context of personal data protection. But, if the draft reaches to the level of law, a regulation or directives that may be issued may address privacy issues.[126]

Thus, in such a situation, issues like what kinds of surveillance cameras we need to install and where (purpose specification); what are the rights of the "data subjects" to the surveillance process and the data collected by the system; how long the footages shall be retained remain unsolved issues in Ethiopia. In turn, though the FDRE Constitution (article 26(3) provides for limitation on

[124] 6Wresearch, *supra* note 122.
[125] CCTV Distributors in Ethiopia,
[126] Interview with Hayalneh Lemma, the Legal Service Directorate Director at Ethiopian Innovation and Technology Minster, 20 April 2021.

right to privacy, where there is no sufficiently precise rules governing limiting the right to privacy through video surveillance, any restriction on video surveillance cannot be legitimate.

In absence of a regulatory framework, law enforcement authorities or other owners of digital surveillance infrastructure may set up a centralized surveillance center where operators can view thousands of video cameras and can abuse the system for illegitimate purposes. As a result, like troubling incidents reported in various countries will most likely happen in Ethiopia too. Besides, private sectors may also use surveillance cameras not only for the sake of maintaining safety, but also to assess employees' performance. Thus, regulation of video surveillance proactively is legislative prudence.

While developing a norm about how surveillance cameras should be used in Ethiopia, it needs to establish a clear public understanding of major issues associated with video surveillance. Among the other things, the need for notification of the surveillance to the public, prohibition or restriction of workplace surveillance, retention period of footages, public access to their data, need for authorization from the regulatory body before installing CCTV system and other privacy safeguarding issues should be explicitly regulated. These issues are usually called as a processing of personal data. In other words, Data processing in practice includes the collection, use, modification, storage/retention, disclosure, and destruction of personal information.[127]

### 4.2.Variables that may be Considered in Building Video Surveillance Code in Ethiopia

The widespread use of video surveillance cameras in major Ethiopian cities and possible encroachment on privacy, necessary calls for an adequate regulatory framework that can address the current and potential dangers of unrestricted use of surveillance tools. The emergence of complex crimes should be tackled through a digital systems, but the law should strike a balance between the need for surveillance and the interest of privacy. Norms create regulatory framework and control methods that establish responsibility and accountability. This section summarizes international norms and best practices that the law revision can consider. Tested international experiences and norms can easily be molded in a way applicable to the Ethiopian situation.

[127] Patricia K, & Adam K, *The International Comparative Legal Guide to: Data Protection 2018*, Global Legal Group Ltd, London, (2018), p.4.

*i. Necessity*

Since video surveillance is one of the means to limit the right to privacy, the principle of necessity should be strictly adhered. Almost all countries that have enacted video surveillance regulatory laws have incorporated the principle of necessity into their legislations. In Canada, the system cannot be used unless there is a 'real, substantial and verifiable' problem that calls for video surveillance.[128] It can only be conducted as a last option in absence of other lesser privacy-affecting mechanisms. In the Netherlands, one of the preconditions to deploy surveillance videos in business organizations is demonstrating the necessity of the system to the Dutch Data Protection Authority.[129] The Surveillance Camera Code of Practice (2013) of the United Kingdom also clearly provides for the mandatory requirements of necessary condition/ pressing need to use surveillance cameras.[130]

*ii. Pre-existing Legal Base*

To protect the right to privacy in the context, there should be sufficiently clear pre-existing rules governing video surveillance. The UK Surveillance Camera Code of Practice (2013) states that, "Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them."[131] In Canada, the law imposes an obligation on the private sectors to develop a policy on the use of video surveillance before starting to conduct the surveillance.[132]

*iii. Operating CCTV for a specific purpose (proportionality)*

To prevent and minimize abuse of the system, "the cameras should only be used for those purposes originally identified when the decision to install them was taken".[133] The progressive expansion of function should be avoided. Therefore, while the CCTV surveillance for the purpose of preventing

---

[128] See Ontario's Freedom of Information and Protection of Privacy Act (FIPPA), section38 (2). See also Municipal Freedom of Information and Privacy Act (MFIPPA), 28(2). See the Personal Information Protection and Electronic Documents Act, 2000(PIPEDA) of Canada.

[129] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/

[130] See The United Surveillance Camera Code of Practice (2013), principle 1. The Data Protection Act 1998 (DPA): data protection principle 2 and 3.

[131] See *Id*, principle 2 &5. And see The Data Protection Act 1998 (DPA): data protection principle 1 &2.

[132] The Canada Personal Information Protection Act and Electronic Documents Act, 2000 (PIPEDA). And see Guidelines for video surveillance in Canada (2015).

[133] Philosopher and criminologist Andrew Von Hirsch, "CCTV and human rights" pp. 3, the last paragraph.

theft or damage to property, and protecting employees and visitors in work place is allowed, it is forbidden to use surveillance cameras to assess employee's performance under the Netherlands CCTV law.[134]

The need for a specific purpose may include limiting the types of cameras required to be deployed and their equipment to the purpose aimed to achieve. For instance, high-resolution cameras can be allowed to read a pamphlet from a mile away. Similarly, cameras are equipped to detect wavelengths outside the visible spectrum. On the same token, cameras allowing night vision/see-through vision detection can be allowed to monitor incidents that may happen in nighttime. Depending on specific needs regulators may allow cameras equipped with facial recognition, or cameras augmented with forms of artificial intelligence.[135]Unless properly regulated otherwise, such capabilities in surveillance technologies would generate incalculable breach of the right to privacy. In this regard, Canada's surveillance law requires limiting the use and viewing range of cameras as much as possible.[136]

*iv. Rights of the Public*

While allowing processing of personal data through video surveillance, certain rights of data subjects such as the right to consent and withdraw the same, right to know, right to access, right to deletion of personal data, and right to complain in case of interference should be specifically covered by video surveillance regulation. In other words, data collectors and processors bear obligations to respect and promote these rights while collecting and processing personal data by using surveillance cameras.

According to the data protection laws of Canada that governs the video surveillance, there should be a clear signals that warn the public regarding surveillance cameras are in use, and "mentioning the perimeter of the surveillance areas, the person responsible for surveillance and his contact

[134] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/

[135] American Civil Liberties Union "what is wrong with public video surveillance" (2021), Available on:https://www.aclu.org/other/whats-wrong-public-video-surveillance.

[136] Public Surveillance System Privacy Guidelines, Office of the Information and Privacy Commissioner, British Columbia, OIPC Policy 00-001, June 21, 2000.

details in case of any queries."[137] This indicates the *public's right to know* what is going on, for what reason and the data collector's obligation to conduct the surveillance transparently. The Netherlands' law also requires signaling about the ongoing surveillance with prominently placed signs and other proper means.[138] In addition, the Surveillance Camera Code of Practice (2013) of the UK, "there must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints."[139]

This principle includes the rights of the public to know and to complain in case of wrong collection and processing of their data. There must be a clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, and used.

Data subjects also have *a right to access to their data* recorded via surveillance cameras. In this regard, the Canada's privacy law regime provides that "the people whose images are recorded should be able to request access to their recorded personal information."[140] Another crucial right of data subjects concerning video surveillance *is the right to consent and withdraw.* Mostly the need for consideration of this right may arise in case of disclosure of personal data recorded by the surveillance cameras. Though the laws in UK, Canada, and the Netherlands declare the need for rules and restricted disclosure of personal data for clearly identified purposes, they do not specifically incorporate the right of the data subject to the consent and withdrawal at time of disclosure.

Finally, the public has the right to complain in case of any wrong act regarding video surveillance process. In this regard, the Data Protection Act 1998 of UK provided for the right to claim compensation when there is damage.[141] The laws in Canada and Netherlands do not directly refer to this right in the specific context of the video surveillance.

---

[137] Ontario's Freedom of Information and Protection of Privacy Act *supra* note 128; Municipal Freedom of Information and Privacy Act supra note 128 Personal Information Protection and Electronic Documents Act *supra* note 128.

[138] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/

[139] See The United Kingdom Surveillance Camera Code of Practice (2013), principle 3 &4. The Data Protection Act 1998 (DPA): data protection principle 6.

[140] See Ontario's Freedom of Information and Protection of Privacy Act *supra* note 128.

[141] The United Kingdom, Data Protection Act (1998).

*v. Retention period*

Videos collected through surveillance systems cannot be retained forever. Depending on the nature of objectives for surveillance, the retention period may vary, but there shall be a time limit. According to section 5(1) of Regulation 460 of FIPPA, and section 5 of Regulation 823 of MFIPPA, the maximum period to retain personal information is one year.[142] Further, the guidelines require the recorded images to be destroyed when they are no longer in use.[143] In some jurisdictions, the period for storing data is very short. The Netherlands, for example, unless dictated by a particular incident that requires a longer time to resolve issues that triggered surveillance, the maximum retention period for footage is four weeks.[144]

*vi. Installation Place*

In the context of privacy, spaces can be understood as an "open air public places", semi-private spaces, and totally/completely private spaces. Since, the degree of privacy individuals need vary, applying surveillance cameras in certain very sensitive areas like washrooms, bedrooms in guest houses, and the like should be restricted or prohibited by law. Such a semi-private spaces are highly sensitive than "open air public spaces such as public roads, parks, and squares, where individuals generally have a lower expectation of privacy."[145] As per the Netherlands law of video surveillance by private sector, cameras should be placed in places where the possibility of threats to privacy is minimal.[146]

*vii. Privacy Impact Assessment*

Before embarking on surveillance, its impact on privacy and possible option that could mitigate adverse effects shall be thoroughly studied. Assessment can be conducted either before or after the commencement of the surveillance. In Canada assessment of the impact of CCTV on the right to privacy is a mandatory requirement.[147] In the UK, in addition to the review of the possible effects

[142] Section 5(1) of Regulation 460 of Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) and section 5 of Regulation 823 of Municipal Freedom of Information and Privacy Act (MFIPPA).
[143] Office of the Information and Privacy Commissioner, Public Surveillance System Privacy Guidelines, British Columbia, OIPC Policy 00-001, (June 21, 2000).
[144] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/
[145] Information and Privacy Commissioner of Ontario, Guidelines for the Use of Video Surveillance (2015).
[146] *Id*.
[147] *Id*, p.18.

of surveillance, the law requires publication of the review report.[148] The Netherlands code of conduct stipulates for assessment the existence of conflict between the employers right to use surveillance cameras and the privacy rights of the employees in advance.[149] If the right to privacy overweighs the employer's right, the system should not be used. Moreover, depending upon the purpose, if surveillance takes longer period of time, it is mandatory to conduct "data protection impact assessment".[150]

The experiences and norms developed in global communities suggestibly would assistive in setting a future Ethiopian video surveillance code. Rules of collection of images and other information, use, retention, disclosure, access, security of personal information collected can be a good resource in designing a legal and institutional framework in video surveillance regulation in Ethiopia.

## 5. CONCLUSION

Though the meaning, nature, and contours of the right to privacy are not uniform in all jurisdictions. the right to privacy is recognized, as a human right, in international and regional human rights instruments, and in almost all constitutions of the global community. The variables for determining privacy depend upon social, cultural, economic, and religious considerations. Despite variation in grounds for delineating privacy, there are common facts in all communities – the existence of matters that cannot be exposed to everyone – private matters that need to be protected. Privacy involves respect to the expectations of private persons that certain personal facts cannot be exposed without voluntary disclosure, including but not limited to personal data, correspondences, family life, premises, and so forth against unlawful and arbitrary interference.

Legal protection of the right to privacy essentially mean guarantees provided by international instruments that shape domestic legislation serving as a model or domesticated in national laws. In some exceptional situations, the right to privacy may be limited when an express and reasonable law that is meant to strike a balance between the public interest for safety and security, and the private interest for non-disclosure of private facts and information provides to do so. The limitation should be necessary and proportional to compelling circumstances.

[148] See The United Kingdom Surveillance Camera Code of Practice (2013), 2&10.
[149] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/.
[150] *Id*.

However, the development of the digital surveillance methods enables invisible intruders to violate the requirements of law. The cheap availability and the possibility to watch remotely has attracted public institutions and private persons to rely on digital surveillance technology. Despite its significance in the fight against terrorism and destructive crimes, extensive use of video surveillance is subject to abuse. Thus, unless properly regulated, the negative effect of video surveillance on the right to privacy is incalculable.

As a member of the global community, Ethiopia not only recognizes the international bill of rights but also shaped its domestic law in light of international human rights pillars, including the right to privacy. Though not comprehensive and adequate enough to accommodate the ever-expanding digital surveillance system, Ethiopia has expressly recognized the right to privacy throughout various legislations. However, the existing Ethiopian laws do not align with the ever-changing lifestyles, economy, politics, and technological advancements. Secondly, the laws do not address sufficient contents of the right to privacy and lack policy frameworks. In Ethiopia, there is no legal framework that can address the emerging digital surveillance technology. Ethiopia needs to enact a comprehensive privacy law that can proactively address potentially dangerous intrusion in private life through remotely controlled video surveillance cameras. The new law should be designed in consideration of international norms, standards, and best practices.

The work points out the need for building video surveillance codes in line with the developed nations. Factors and possible variables that may be considered in setting guidelines for video surveillance regulation are briefly pointed out.

# The Requirement of Leave without Pay to Run for Election in Ethiopia: A Subtle Deprivation of Civil Servants or Levelling a Playground in Quest for Fairness?

Nesredin Ahmed*

**Abstract**

The article assesses the critic against the new Electoral Law (Proclamation No.1162) of 2019, which included controversial rules that require civil servants to get leave without pay as a condition to run for elected offices. There was a hot debate against the new rule. Opposition parts and civil servant candidates argued that the poorly paid Ethiopian civil servants cannot withstand effects of leave without payment during the candidacy. Ethiopian civil servants often live from pay to pay would not choose to cost themselves their family in aspiration to serve the public. This is validly argued as a subtle deprivation of right to be elected, which is guaranteed by the FDRE Constitution. The deprivation is also contrary to the accepted international election norms, international election principles and standards. This article examines the propriety of indirect limitation on rights of Ethiopian civil servants in light of international human rights treaties, international election rules, and experiences other nations by primarily relying on the doctrinal research methodology.

**Keywords:** Civil Servants, Election norms, Election Board, Human Rights, subtle deprivation

## 1. Introduction

In a democratic nation it appears for granted that every citizen that is eligible to run for public offices has unfettered constitutional right to elect and be elected in periodic elections. Running for elected offices is a political right that is guaranteed in national and international levels. Needless to say, civil servants, as citizens, have right to elect and be elected. But the new election law (Proclamation No.1162/2019) practically restricts, if not taken as a ban, Ethiopian civil servants right to take part in periodic election. Among others, the Proclamation requires civil servant candidates to vacate their employment position as a condition to run for elected offices.[1] Given the

*LL.B, MA The author is grateful to Dr. Tesga Andulalem for his unreserved assistance in editing the article to the level of publication in EJoLS. The author is responsible for errors or idea expressed in the article.

[1] Ethiopian Electoral, Political Parties Registration and Election's Code of Conduct Proclamation 2019, Proclamation No. 1162/2019, FDRE NEGARIT GAZETTE 25th Year No. 97 Oct. 2019, A.A., art.33 (1)(b) .

current economic condition of Ethiopian civil servants, is it possible to manage election campaign and finance private life without a pay in aspiration to serve the public? Is the requirement to vacate employment position to run for election legal and aligns with international norms?

While it is the sovereign right of each nation to determine how to manage its electoral process, UN Member States have agreed to comply with a set of responsibilities and commitments to protect and promote their citizens' election related rights (Resolution 68/164).[2] The obligation to effectively enforce the right and ability to stand for election as a candidate, without any discriminatory ground such as residency, education, position or any other arbitrary ground, is internationally guaranteed.[3] For instance, the Universal Declaration of Human Right (UDHR), which is commonly accepted as international customary law under article 21, recognizes the importance of periodic and genuine elections which shall meet the requirement of universal and equal suffrage;[4] whereas article 25 of the ICCPR states that the rights to vote and to be elected should be conferred to citizens without discrimination based on race, color, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status.[5] At the regional level, though the African Charter on Human and Peoples' Rights does not explicitly mention the rights to vote and to be elected, it later adopted African Charter on Democracy, Election and Governance which contains relevant provision that requires state members to the charter to promote democracy and recognize popular participation.[6]

Generally, it takes a couple of weeks from candidacy to the point of declaration of election results within which a civil servant candidate makes no employment income.[7] This scenario is exacerbated

[2] United Nation, General Assembly (18 December 2013), Strengthening the role of the United Nation in enhancing periodic and genuine elections and the promotion of democratization', A/RES/68/164, (21 February 2014) 1-5

[3] Office of the High Commissioner of Human Right, 'General Comment No. 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service (Art. 25): 12/07/96. CCPR/C/21/Rev.1/Add.7, General Comment No. 25. (General Comments)'.

[4] Universal Declaration of Human Right 1948, art.21.

[5] International Covenant on Civil and Political Rights1966, art.25.

[6] African Charter on Democracy, Elections and Governance 30 January 2007, art.4(2).

[7] For instance, in accordance with the schedule of 2021 election that was released on February 17/2021 by the National Electoral Board of Ethiopia (NEBE), the election campaign was started on February 15 and continued up to May 30 for the election that was held on 29th August. In accordance with the new law a civil servant who chose to run for election can do it only after vacating the office with no pay.

by the low income of Ethiopian civil servants, which denies the opportunity to participate in the election which may amount to a ban on exercising their right to be elected. It is worthwhile to investigate whether an action amounts to a violation of the enjoyment of the right to be elected in light of international obligations derived from international human rights instruments and constitutionally guaranteed. This short article exposes how the new election law subtly encroaches the rights of civil servants to run for elected office in Ethiopia. It is worthwhile to investigate whether these requirement amounts to a violation of the enjoyment of the right to be elected in light of international obligations derived from international human rights instruments and the FDRE Constitution. The next section of the paper introduces principles of democratic election briefly. The third section of the paper provides a general overview of the right to be elected of civil servants and legitimate restrictions that could be imposed on the right. This will be followed by the fourth section that examines the right to be elected of civil servants from a comparative perspective by focusing on the experience of Australia and Canada. The fifth section of the paper analyzes the right to be elected of civil servants in Ethiopia in light to international standards and comparative experience. Finally, the paper winds up by providing conclusionary remarks.

## 2. Principles of Democratic Election

There are international common standards and principles that need to be observed as binding election standards in conducting genuine democratic elections. These standards are applied by most of the international community and can be grouped into binding and non-binding ones. The binding election standards are norms that developed through treaties and international custom as a binding international election standard for undertaking democratic elections. In contrast, non-binding international standards are incorporated in non-binding sources of public international law like resolutions and declarations. Essential principles recognized in these sources include universal and equal suffrage, secrecy of the vote, the right to vote and to be elected, genuine election, free and fair election, the principle of inclusiveness and the principle of non-discrimination.[8] The following are some of the major democratic election principles:

[8] Nils Meyer-Ohlendorf and Avery Davis-Roberts, 'The Carter Center Democratic Reporting International, Strengthening International Law to Support Democratic Governance and Genuine Election'(April 2012),1-65.

### a. Universal and Equal Suffrage

Universal suffrage is one of the essential components of democratic election that guarantees the right to vote and to be elected to all eligible citizens without discrimination. However, it not absolute. Although every state can determine who is eligible to participate in an electoral process, the right to vote and to be elected in a genuine election must not be subjected to discriminatory or unreasonable conditions. In other words, the universal and equal suffrage right "may not be suspended or excluded except on grounds which are established by law, and which are objective and reasonable."[9]

While this criterion applies to all election procedures, it is especially important in the areas of electoral system and boundary delimitation, voter registration, voting operations, and vote counting.[10] It demands that each vote given equal weight, in applying "one person, one vote" rule.[11] Also Electoral district delineation should be determined on an equal basis or in such a way that the right to fair access to the polling station is not impaired. In terms of right to vote, all qualified citizens should have an equal opportunity to run for office, and candidates should not take advantage of unfair advantage.[12] The requirement to apply equal weight to each vote is recognized under the UDHR, ICCPR, and ICERD. For example, in accordance with ICCPR the "principle of one person, one vote, must apply, and within the framework of each state's electoral system, the vote of one elector should be equal to the vote of another." [13]

### b. The Principle of Inclusiveness

Internationally recognized civil and political rights require democratic elections must be inclusive of all citizens who wish to participate in election, and the principle of non-discrimination demand states to ensure inclusive elections in order to guarantee fair electoral contest.[14] The principle of inclusiveness in turn requires the rules not to be unreasonably restrictive.[15] Failure to respect the

---

[9] Tuccinardi *et al*, (ed) *International Obligation of Elections: Guidelines for Legal Framework*, (2014) 42, https://www.idea.int/sites/default/files/publications/international-obligations-for-elections.pdf

[10] The Carter Center, Identifying Obligations for Democratic Elections: Narrative of Obligations`, Draft of 2009(2009), 14 https://www.cartercenter.org/resources/pdfs/peace/democracy/des/narrative-of-obligations.pdf.

[11] Florina Baskievska Andreevska *Protection of the Voting Right by the Administrative Courts*, KNOWLEDGE-INT'L J. vol. 48 No. 1 (2021) 5-6

[12] *Id*.

[13] OSCE/ODHIR, *Guidelines for Reviewing a Legal Framework for Elections* (2ndedn, Office for Democratic Institutions and Human Rights (OSCE /ODIHR, 2013)19.

[14] *Id* at 11

[15] *Id*.

concept of inclusivity also undermines the electors' freedom to select among those who aspire to represent them by arbitrarily denying them that choice.[16] Therefore, electoral processes and legal frameworks of election should meet the principle of inclusiveness.

### c. Free and Fair Elections

There is no common understanding of what a free and fair election is and of its requirements. Generally speaking, free election connotes free expression of the people's will as well as free public political engagement, as enshrined in the human rights documents such as the UDHR and the ICCPR. In order to participate in an election, there must be no intimidation. Obstacles to full participation, as well as other key rights in democratic elections, such as the right to vote, must be addressed.[17] Furthermore, all elements of the electoral process must function without undue interference.[18] This indicates that any measure including the legal framework that has the effect of discouraging political participation must be avoided. Likewise, elements of fair election are found in international human rights instruments; mainly under UDHR article 2 and 21 (3)[19] and ICCPR article 2 and 25 (b).[20] Equal, universal, nondiscriminatory suffrage is one of these criteria. A criterion for eligibility that is arbitrary or excessive is prohibited. In general, the conduct of many national elections is evaluated as a free and fair election by observing the legal framework, institutional framework, and electoral processes.

### d. Equality before the Law and Absence of Discrimination

The right to enjoy human rights, free from discrimination, is widely recognized at the international and regional levels. The term “discrimination” is fact specific and determined contextually but it inherently implies distinction or restriction that based on anyone or more of the grounds that are specified in the Covenant which have the effect of nullifying or impairing the enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms.[21] The right of equality and absence of discrimination is presumed when other fundamental human rights are respected throughout the electoral process. The State is obligated to observe both its’ ‘negative duty’ to

---

16 *Id*. at 12 .
17 United Nation (n2)22.
18 *Id*.
19 Universal Declaration Human Right (n 4).
20 International Covenant on Civil and Political Rights (n 5),arts.2 and 25(b).
21 United Nation, ‘Human Rights Committee, General Comment 18, Non-discrimination (Thirty-seventh session, 1989), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 at 26 (1994).’ par.1.

refrain from engaging in discriminatory manipulations and its 'positive duty' which imposes duty take measures that would remove of obstacles for the equal enjoyment of such rights, including the adjustment of domestic legislation.[22]

Discrimination can be direct or indirect. Direct discrimination occurs where a provision specifically treats a certain group or organ on the basis of either a listed or an unlisted grounds, and indirect discrimination occurs where certain requirements, conditions or practices, while appearing neutral, actually have an effect or result that is unequal or that disproportionately affects a particular group or individuals. To illustrate, if electoral law clearly establishes different eligibility criteria for citizens and non-citizens, or for civil servants and non-civil servants it may be considered as an instance of direct discrimination. The treatment, on the other hand, may be similar, but its effects may be unequally distributed. For example, if the law provides equal right to be elected for men and women, it may result indirect discrimination. Both direct and indirect discrimination seems to be implicitly prohibited under article 25 of ICCPR. Yet, what makes a differentiation reasonable and unreasonable is not defined clearly, but grounds of unreasonable discrimination are listed illustratively and open for inclusion of similar factors. As such, reasonable requirements or qualifications for exercising the right to vote and to be elected do not amount to discrimination. A differential treatment based on reasonable and objective criteria does not amount to a prohibited discrimination within the meaning of article 26 of ICCPR.

### 3. Ethiopian Civil Servants Right to Run for Election and Legitimate Limitations

The unfettered right to vote and elected is one of the most important elements of democratic elections. At its core, it implies that national legislation should provide appropriate procedures for party and candidate registration providing equal opportunity for all political views and groups, with no undue limitations.[23] Every citizen must have the right and chance to run for office on an equal footing with other citizens, and registration procedures should not be too onerous.[24] Existence of equal rights are not enough; equal chance to enjoy or exercise those rights is essential, and states have a positive duty to enable or take affirmative actions to ensure that equal rights are

[22] Office of the high Commissioner of Human Right 'CCPR General Comment No. 28: Article 3 (The Equality of Rights between Men and Women)' 2000, par.3.

[23] Election observation and democratic support, *Compendium of International Standards for Elections* (4thedn, European Union, 2016) 25.

[24] *Id*.

enjoyed. This right can only be limited by objective and reasonable legal criteria that are not in conflict with international obligations. Equal opportunity to vote and be elected also requires the state to 'take effective measures to ensure that all persons entitled to vote and be elected can exercise that right'.[25]The CCPR authoritative interpretation states further that 'no person should suffer discrimination or disadvantage of any kind because of that person's candidacy'.[26] The obligation that all people have an equal chance to vote and to be elected forbids '*de jure* or *de facto'* discrimination as well as unjustified limitations that might lead to inequities.[27] Yet, the exercise of electoral rights is not absolute and may be subject to reasonable limitations.

### 3.1. Grounds for Limitation

Although there are international common standards on candidacy qualifications and elector eligibility, as indicated in the various constitutions and electoral laws of states around the world, they may vary in accordance with the historical and political factors specific to each State.[28] Hence, for the purpose of this article, the grounds of limitations are classified in to the following four major doctrines: (a) The doctrine of incompatible office; (b) Political neutrality; (c) Conflict of interest; (d) Individual capacity.

#### A. Doctrine of Incompatible Office

The concept of incompatible office is a common law legal doctrine which prohibits an individual from holding two positions at the same time which are deemed "incompatible."[29] This is usually determined by looking at the nature and responsibilities of the respective positions and check if there is a policy reason that justifies prohibition.[30] Further, incompatibility grounds may vary based on the public policy of the concerned state and its legal system. General Comment 25 on article 25 of ICCPR, paragraph 16 elaborated this as "If there are reasonable grounds for regarding certain

---

[25] Office of The High Commissioner of Human Right 'General Comment No. 3: Article 2 (Implementation at the National Level)' 1, par.1.

[26] Office of The High Commissioner of Human Right, 'General Comment No. 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service (Art. 25): 1996. CCPR/C/21/Rev.1/Add.7, General Comment No. 25. (General Comments)' par.15

[27] Tuccinardi and Wally (n 9) 41.

[28] Council of Europe/European Court of Human Rights 'Guide on Article 3 of Protocol No. 1 to The First Protocol to the European Convention on Human Rights: Right to Free Elections' (n 9) 16.

[29] Compatibility ethics-Muni-Newsl-Summer 1 <https://nysba.org/app/uploads/2020/03/Compatibilityethics-muni-newsl-summer04.pdf> accessed 6 March 2021.

[30] *Id.*

elective offices as incompatible with tenure of specific positions (e.g. the judiciary, high-ranking military office, public service)…"; 'The grounds for the removal of elected office holders should be established by laws based on objective and reasonable criteria and incorporating fair procedures.'[31] Therefore, when incompatibility is proved, the right to be elected may be limited.

### B. Political Neutrality

Due to statutory election laws or public policy considerations, certain public officials may be obliged to remain politically neutral. As provided in circulars of different countries such as Circular 09/2009,[32] Circular 4/2002[33] and Circular 26/04;[34] the restrictions placed on civil servants in relation to politics and political activity are designed in order to ensure confidence in the political impartiality of the Civil Service, and to ensure that a civil servant must not do anything that could give rise to a perception that his or her official actions are in any way influenced or capable of being influenced by party political motives. Many legal systems stipulate that judges, and other members of the staff of 'public-law institutions and public undertakings must be politically neutral.[35] The concept of an impartial and competent public service capable of providing independent policy advice and implementing government policy without political consideration necessitates public servants be nonpartisan, and that they be perceived as such by both the current government and the people with whom they associate. If public servants were recognized as partisans as a result of their visible political activity, their allegiance to the government of the day could be called into question. Similarly, their impartiality in carrying out their duties could be questioned by people who need their service and do not share their political views. In the work of Niroja Arulananthan (2018),[36] the author found that ethic of neutrality has the potential to cause conflicts of interest and recommended that 'there should be legislation and policy change to avoid

---

[31] CCPR General Comment 25' (n 5) par.16

[32] A Dhuine Uasail, 'Circular 09/2009: Civil Servants and Political Activity'. https://circulars.gov.ie/pdf/circular/finance/2009/09.pdf (accessed July 25, 2022).

[33] AChara, 'Circular 4/2002 -Standards in Public Office Act 2001' <http://www.irlgov.ie/finance>. (accessed July 25, 2022)

[34] A Dhuine Uasail, 'Circular 26/2004:- The Civil Service Code of Standards and Behaviour'. https://circulars.gov.ie/pdf/circular/finance/2004/26.pdf (Accessed July 25, 2022).

[35] Council of Europe/European Court of Human Rights 'Guide on Article 3 of Protocol No. 1 to The First Protocol to the European Convention on Human Rights: Right to Free Elections' (n 9)21.

[36] Niroja Arulananthan, 'An Evaluation of the Ethic of Neutrality in the Ontario Public Service A Thesis on The Conflict of Interest Process and Its Impact on Public Servants' (A thesis submitted in conformity with the requirements for the degree of Masters of Arts, Graduate Department of Leadership, Higher, and Adult Education, University of Toronto 2018).

ambiguity of what is neutrality and extent of neutrality in a way it ensure that burden posed by the ethic of neutrality on political participation of public servants could be reduced. The researcher agrees with the stand of this author and related with the issue at hand in the comparative perspective.

### C. Conflict of Interests

There is no common definition of conflict of interest. It may be explained as " […] a situation in which a public official has a private or other interest which is such as to influence, or appear to influence, the impartial and objective performance of his or her official duties."[37] Some governmental posts, such as judges, prosecutors, police officers, members of election commissions, tax authorities, or members of the defense forces, may require candidates to resign from their jobs before campaigning, for reasons of impartiality which might affect a candidate's standing.[38] The authoritative interpretation of ICCPR on article 25 by HRC tacitly recognizes that the state parties to the covenant may take certain measures to avoid conflict of interest.[39] Restrictions may also apply if they are mandated by law and are required in a democratic society for national security or public safety, the prevention of disturbance or crime, the preservation of health or morality, or the preservation of others' rights and freedoms.[40]

### D. Individual Capacity

Individuals who want to participate in an election need to have capacity. The requirements concerning the capacity of the candidate may vary from one country to another and the various systems can pursue different thresholds. The capacity requirements can be age, residence, nationality, having mental capacity, judicially not interdicted person.[41] 'The Venice Commission

---

[37] Quentin Reed Governance and Anti-Corruption Consultant, 'Sitting on the fence: Conflicts of interest and how to regulate them' (Anti- Corruption Resource Centre 2008)7.

[38] Maurer D and Ardita, *Using international standards in elections: Council of Europe handbook for civil society organizations* (1st edn, Council of Europe 2016) 49.

[39]'. General Comment No. 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service (Art. 25) : . 12/07/96. CCPR/C/21/Rev.1/Add.7, General Comment No. 25. (General Comments' par.16 <https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2025.pdf> accessed 1 January 2021.

[40] The Inter-Parliamentary Council, 'Declaration on Criteria for Free and Fair Elections unanimously adopted by the Inter-Parliamentary Council at its 154th session (Paris, 26 March 1994' art.3 (7) <http://www.ipu.org/cnl-e/154-free.htm>.

[41] Maurer and Ardita (n 38) 48–49.

2002 Guidelines,[42] provides a list of basic "reasonable restrictions" concerning: age, nationality and residence and examples of such restrictions are also provided in the Final Report of the OSCE/ODIHR Election Observation Mission to the 2013 Presidential Election in Georgia.[43] It has also been common to place restrictions on the right to be elected based on mental incompetence or a criminal conviction for a serious crime, which may only be imposed by a court ruling.[44]

### 3.2. Reasonableness of Limitation

The grounds of limitation on the right to be elected may be divided into "reasonable" and "unreasonable" restrictions. The existence of the aforementioned justifications does not imply that limits on the exercise of the rights to be elected are reasonable. Meeting the requirements, reasonability test is necessary for governments to fulfill their obligations to respect and ensure electoral related rights. The major test for assessing the reasonableness of limitation is called proportionality and it encompasses requirements of legality, presence of legitimate aim and necessity discussed below.

#### A. Legality

Any limit on the right to be elected must be backed by the legal framework for elections, which must be explicit, precise, and established by legislation in order to ensure clarity and predictability. It must be equitably enforced and implemented without bias.[45] The legal framework should clearly state when a person's suffrage rights may be limited or to what degree, and such limitations must be consistent with the existing constitutional framework. 'Any restriction or limitation on the right to elect or be elected must be exceptional and needs to be examined and clearly justified.'[46] The reasons for the removal of elected office holders should be stipulated by legislation based on objective and reasonable criteria and embracing fair processes, according to the HRC's authoritative interpretation of ICCPR article 25.[47]

---

[42] Council of Europe, 'European Commission for Democracy Through Law (Venice Commission)guidelines'2002, sec.1.
[43] Maurer and Ardita (n 38) 49
[44] *Id.*
[45] *Id* at 29
[46] OSCE/ODHIR 'Guidelines for Reviewing a Legal Framework for Elections' (n 37) 19
[47] Council of Europe/European Court of Human Rights Guide on Article 3 of Protocol No. 1 to The First Protocol to the European Convention on Human Rights: Right to Free Elections' (n 9) 15.

### B. Legitimate Aim

Under international law, the ideal of equality and non-discrimination does not imply that all inequalities between individuals are forbidden. As such, governments may be allowed to discriminate provided they have a compelling basis to do so. This is known in legal terms as 'objective justification'. Discrimination that is justifiable is not considered as unlawful discrimination. Distinctions are justified and hence legal if they have a valid goal, such as affirmative action to address factual inequities, and are reasonable in light of that goal. In principle, the right to be elected is universal, but exceptionally, the right may be restricted for a purpose that is legitimate. Although governments have a considerable leeway in determining the extent of restriction on the right to vote and be elected, they must ensure that it serves a legitimate goal.[48] When a government fails to justify its activities with reasonable and objective standards, the activity ceases to be justified and becomes discriminatory.[49] Majority age and mental ability standards, for example, are not discriminatory because they are designed to assure decision-making competence. To avoid conflicts of interest or political impartiality, public officials may be subjected to additional criteria to run for office. However, the legitimate aim does not justify excessive measure.

### C. Necessity and Proportionality

The goal or reason for the discrimination must be fairly balanced against the disadvantages suffered as a result of the discrimination. This implies that it must be appropriate and necessary. Otherwise, it will be difficult to defend differential treatment if there are better and less discriminating methods of doing things. While no country in the world has entirely unrestricted suffrage, the limit must be acceptable.[50] Limitations to states' margin of appreciation could be considered through evaluating whether conditions or restrictions respect the principle of proportionality. Broad legislative rules that limit the suffrage rights of broad categories or groups of persons without taking into account the specific circumstances of each instance are incompatible with the concept of proportionality; hence any restriction must be implemented narrowly.[51] 'The

[48] Maurer and Ardita(n 38) 42.
[49] *Id. at* 29.
[50] International Covenant on Civil and Political Rights (n 5).
[51] OSCE/ODHIR, Guidelines for Reviewing a Legal Framework for Elections'(n 37) 20.

proportionality test evaluates that the limitation is proportionate to the extent necessary for the exigency of the situation.'[52] Regarding the proportionality test, General Comment 25 provides that 'if a candidate is required, to have a minimum number of supporters for nomination, this requirement should be reasonable and not act as a barrier to candidacy.'[53]

However, any legally mandated minimum thresholds that parties or candidates must meet in order to qualify for election must not be used to purposefully exclude certain political parties, national minorities, or groups of people.[54] Unreasonably high criteria, for example, may preclude parties from getting elected. Reasonable limits on the exercise of election related rights shall be applied solely in good faith in order to fulfill duties to protect and safeguard electoral related rights.[55]

The fact that limits on the right to run for office have a valid goal does not make the ground for limiting reasonable, if the consequence of the restriction renders that right ineffective.[56]Any limit on electoral rights should not prevent specific people or groups of people from participating in the country's political life.[57] The cumulative reading of article 5 (1) of ICCPR and the General Comment 25 paragraph 27: clarify that 'any act of interpretation may not destroy or impair or should not diminish the rights and freedoms guaranteed by the Covenant to a greater extent than is provided for in the Covenant.'[58]The Siracusa principle also states 'a restriction to the Covenant must not jeopardize the essence of the right in question.'[59]

### 4. Right to be Elected of Civil Servants and Its Limits: Comparative Perspective

As a principle, every citizen must have the right and the opportunity to be elected in equal conditions with other citizens and registration procedures should not be so difficult as to inhibit candidacy.[60] Right to be elected is an internationally recognized political right which demonstrates

---

52 The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' <https://www.jstor.org/stable/762035>.

53. CCPR General Comment 25' (n 3) par.17.

54 Maurer and Ardita (n 38) 27.

55 Constitution of the Federal Democratic Republic of Ethiopia (n 11).

56 Council of Europe/European Court of Human Rights 'Guide on Article 3 of Protocol No. 1 to The First Protocol to the European Convention on Human Rights: Right to Free Elections' (n 9) 21.

57 Maurer and Ardita (n 38)19.

58 CCPR General Comment 25' (n 5) par.27.

59 The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights'. https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf.

60 EODS: Election Observation and Democratic Support, https://www.eces.eu/en/posts/eods-ii.

that genuine election must be inclusive for all citizens who want to exercise their right to be elected and an anti-discrimination norm obliges states to provide inclusiveness in electoral processes, mainly in fair electoral competition. Article 25 of ICCPR and its authoritative interpretation GC 25 provides the universality of right to be elected. ICCPR Article 25: "Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions: (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors."[61] Similarly, General Comment 25 paragraph 15: provides that any person who is qualified to be candidate must not be disqualified by unreasonable or discriminatory requirements by stating that "no person should suffer discrimination or disadvantage of any kind because of that person's candidacy." [62] Moreover, both binding and non-binding international and regional elections standards or principles and guidelines that promote genuine democratic election which have evolved from protocols, declarations, treaties, and other international and regional instruments that safeguard democracy and human rights are applicable for right to be elected of civil servants. The formal applicability of the standards mentioned above to a particular country depends upon its accession to such treaties whether the country has signed on to the treaty standards or not, and its normative commitment to foster the promotion of, and support for, these international and regional election standards.[63] Similar to others, civil servants have universal and equal suffrage right to be elected in principle. However, the right to be elected is not an absolute right and exceptionally, can be restricted under certain circumstances.

Notably, restrictions on political participation can only be justified in terms of preventing some greater evil. In other words, the ban on political participation of civil servants is regarded as desirable only if it forestalls some kind of danger than that of restrictions on political participation.[64] Civil servants must uphold high standards of integrity and the reputation of the

[61] International Covenant on Civil and Political Right (n 5).

[62]'*Id.* Par.15.

[63]Fabio Bargiacchi and others, *Using International Standards Council of Europe Handbook for Domestic Election Observers* (Service for the Production of Documents and Publications (SPDP), Council of Europe 2013) 12–16 <France http://www.coe.int/t/dgap/eap-facility/>.

[64]Leon D Epstein, 'Political Sterilization of Civil Servants: The United States and Great Britain, Vol. 10, No. 4 ASPA (1950)282.

service; as a result, they must exercise their role 'properly and act lawfully', 'honestly, and loyally' without seeking personal gain. Thus, they must have a number of principles to abide by. In order to ensure compliance with these civil servants' ethical standards, states have a wide discretion to enact different codes of conducts, regulations, guidelines and rules that provide criteria of eligibility to stand for election. As mentioned previously, the grounds of limitation on the right to be elected in general, restrictions on the right to be elected of civil servants may vary between countries. However, the main considerations are avoiding conflict of interest, prohibition of misusing administrative resources during election, capacity requirements, issues of incompatibility of the job, and issues of political neutrality.

For the purpose of comparison, the author has chosen Australia and Canada because of their better practice in managing the balances between the two conflicting measures: avoiding unreasonable restrictions on political participation of civil servants and preservation of political neutrality, impartiality, loyalty, integrity and avoiding any conflict of interest. For example, the arrangement under Australian legal framework for election classifies political participation in to three levels; Federal elections, State elections and Local election, which is projected to identify level of participation that more vulnerable to conflict of interest. Federal election is claimed to be more open for conflict of interest and designed with more restriction. For similar reason Canada classifies civil servants into three groups. Similarly in Ethiopia, the author believes that level of participation and status of participants has great relation with conflict of interest. For instance, a minister at federal level and a teacher at elementary school are not similarly engage in politics and hence that both countries could be a model for Ethiopia.

**a. Australia**

Under Australian legal system civil servants political participation and any conflict of interest that could arise comprehensively is governed by, Commonwealth of Australia Constitution Act, The Australian Guidelines on Official Conduct of Commonwealth Public Servants Act 2008 (PSA), Parliament of Queensland Act 2001 (PoQA), Local Government Electoral Act 2009 and Act 2011 and Electoral Act 1992.[65] The arrangement under Australian legal framework for election classifies political participation in to three levels; Federal elections, State elections and Local

[65]Public Service Commission, 'Circular No. 03/14 Public sector employees contesting elections'.

election. Accordingly, public servants in Australia can participate in politics, but with some restraints as to avoid conflict of interest based on their level of participation. The Code of Conduct of Public Servants set out the standards of conduct required of public and allows public servants to "become members of, or hold office in, any political party" taking precautionary measures to avoid a conflict of interests including campaign activities. For instance, public servants should make clear that they are not there in their official capacity, and they should not use official facilities for their political activities. Regarding Federal Election, Civil servant can participate in Federal election if they are not among a person holding 'any office for profit under the Crown' and if they are not disqualified by other ground provided under section 44 of the Constitution. If they are the holder of any office for profit under the crown candidates should resign their public employment prior to nominating for election.[66]

In state election, as principle there is no need of resignation but exceptionally those public servants whose role is listed under section 67(1)(a-r) of the Parliament of Queensland Act 2001 should resign and under section 66 a public sector employee must be on leave (either paid or unpaid) for the duration of the election period.[67]

With respect to local election, public sector employees are not required to resign to contest a Local Government election. However, Public service employees have an obligation to resolve any conflicts between their public service duties and other interest in favor of the public interest.
The Australian Guidelines on Official Conduct of Commonwealth Public Servants says that if a public servant is playing a significant part in a political campaign, there is potential for a conflict of interests. Therefore it imposes two duties on public servants: duty to make clear that they are not there in their official capacity and duty not to not use official facilities for their political activities.

### b. Canada

From 1979 to 2006, there was considerable disagreement about the political neutrality and fundamental political rights of public servants in Canada which some key court decisions and, the

[66] 'Commonwealth of Australia Constitution Act' s44 <https://www.legislation.gov.au/Details/C2013Q00005> accessed 21 March 2021.
[67] 'Parliament of Queensland Act 2001' 107

D'Avignon committee call for the amendment of the Public Sector Ethics Act (PSEA) gave public servants a greater liberty to engage in political activities and led the Public Servants Commission (PSE) to strike appropriate balance between the political neutrality and the political rights of public servants.[68] The widespread prohibitions contained in the PSEA, which, for the most part, applied in the same manner to all employee categories and levels, were therefore considered to be excessive and as a remedy, the D'Avignon Committee recommended in 1979 that the public service be divided into three groups for the purpose of determining employees' rights to political participation but the proposal was not accepted at that time. Changes to the political rights provisions of the PSEA were finally made in 2003, when Parliament adopted the Public Service Modernization Act. Therefore now, according to the Canadian Public Service Employment Act, public servants are permitted to engage in political activity as long as they can perform their duties in a politically impartial manner.

## 5. Civil Servants' Right to Run for Election in Ethiopia

Legal frameworks for elections do not have the same old history as the old age of the modern Ethiopian state. The country's first Constitution, enacted in 1931, established a parliament of two chambers: the 'Chamber of Senate, elected by the King from nobility and local chiefs, and the 'Chamber of Deputies.[69] More than using the word election, the Constitutional provisions of 1931 did not set rules regarding provide election and electoral laws. The Revised Constitution of 1955 declared the right to vote to the Chamber of Deputies, but the Chamber of Senate was elected by the Emperor.[70] The undertaking of election for chamber of deputies did not alter existing relations of power because of the strict candidacy qualifications assured the dominance of the landowner as the law requires owning moveable or immovable property or requires the candidate to pledge equivalent money not less than 1000 and 2000 Ethiopian Dollars.[71] Following the overthrow of the Emperor, the Provisional Military Administration Council (PAMC) came with a socialist ideology

[68]Luc Juillet and Ken Rasmussen, *Chapter 5.Struggling to Defend Political Neutrality*: 1979-2006', *Defending a Contested Ideal : Merit and the Public Service Commission, 1908-2008* (University of Ottawa Press 2017).133ff.

[69] Constitution of Ethiopia1931 art.30.

[70]Constitution of Ethiopia 1955, art.95.

[71]Gezahegn Gashaw, 'The need to reform electoral law of Ethiopia' (a thesis submitted to the school of graduate studies of Addis Ababa University in partial fulfillment of the requirements of the degree of masters of laws in Constitutional and Public law, Addis Ababa 2018) 46.

in which civil and political rights had no place. This period was characterized by the absence of electoral laws and institution of election until the 1987 Constitution[72] which guaranteed election related rights under articles 3 and 4, and Proclamation No.314/1987 which was enacted to promote the Constitutional promise. The Proclamation under article 2 (2) also established the Electoral Commission. However, the regime fell down before implementing it and a transitional charter was adopted subsequently.[73]

The 1991 Transitional Charter declared the to respect human rights and promised peaceful democracy. Regional as well as federal assemblies were carried out from 1992-1994 with little competition among rival parties and adopted a new set of electoral rules that were incorporated in the FDRE Constitution. The first electoral law (Proclamation No. 11/1992) was enacted in accordance with the transitional charter. This law later amended Proclamation No. 64/1993 provided detailed provisions on electoral matters, including the establishment of national, regional and woreda council members' election commission including the National Electoral Board.[74] Currently, the FDRE Constitution and other laws adopted subsequently hold rules that meant to regulate election process, including the right of civil servants to run for government offices. As defined in the Ethiopian Electoral, Political Parties Registration and Election's Code of Conduct a civil servant is:

> […] an individual who has been employed as a permanent staff by the federal or regional government offices; however, it does not include ministers, state ministers and other similar level appointments at the federal and regional level as well as members of the House of Peoples' Representatives, Regional Councils and House of Federation.[75]

A civil servant therefore is any permanent employee of either federal or regional government other than persons holding elected offices, including but not limited to ministries, state ministries and other persons who are appointed either by regional or federal governments. Further, it is important

---

[72] Constitution of Ethiopia 1987, arts.3 and 4<https://chilot.files.wordpress.com/2011/04/1987-ethiopian-constitution1.pdf> accessed 17 March 2021.

[73] Gezahegn Gashaw (71 )

[74] Ethiopia Electoral Law Proclamation 1993, Proclamation No. 64 of 1993). <http://ilo.org/dyn/natlex/natlex4.detail?.

[75] Ethiopian Electoral, Political Parties Registration and Election's Code of Conduct Proclamation, (n1), Art. 2(29)

to note the obligations of civil servants is stated under the Federal Civil Servants Proclamation No.1064/2017 including the obligation of loyalty, impartiality; political neutrality, confidentiality, duty to avoid conflict of interest and others are related general duties.[76]

### 5.1. The Right to be Elected of Civil Servants under the FDRE Constitution

Chapter three of the FDRE Constitution of 1995 declares a list of fundamental rights and freedoms that impose limitations on the power of government.[77] Among others, the Constitution guarantees citizens right to elect their representative at all levels of government. Specifically, the FDRE Constitution provides:

> Every Ethiopian national, without any discrimination based on colour, race, nation, nationality, sex, language, religion, political or other opinion or other status, has the following rights:
>
> (b) On the attainment of 18 years of age, to vote in accordance with law;
>
> (c) To vote and to be elected at periodic elections to any office at any level of government; elections shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors.[78]

Article 38 of the FDRE Constitution does not leave any room for discrimination and provides an open-ended list of prohibited grounds of discrimination when recognizing the right to vote and elected in Ethiopia to all citizens "[…] without any discrimination based on color, race, nation, nationality, sex, language, religion, political or other opinion or other status." The phrase, "other status," includes civil service. As provided in the Proclamation No.1162/2019 "Civil Servant" is A "status," on the basis of which one cannot be prohibited to elect or be elected. Therefore, any unjustified discrimination based on being of a 'Civil Servant' is constitutionally wrong.

The Constitution conveys a clear message that both civil and political rights incorporated therein to be applied in accordance with international standards; particularly, in a manner conforming to the principles of the Universal Declaration of Human Rights, International Covenants on Civil and

[76] Federal Civil Servants Proclamation 2017, Proclamation No.1064/2017, art.66.
[77] FDRE Constitution Proclamation art. 38.
[78] *Id*.

Political Rights and other international instruments adopted by Ethiopia.[79] Therefore, the international election standards that are stipulated under article 25 and other relevant provisions of ICCPR and article 21 of UDHR and other international instruments are reaffirmed by the Constitution. Hence, 'any law, customary practice or a decision of an organ of state or a public official which contravenes the international election standards shall be of no effect.'[80] Moreover, as per article 27 of the Vienna Convention on the Law of Treaties, "A party may not invoke the provisions of its internal law as justification for its failure to perform a treaty."[81] Therefore, in principle, any domestic law that contravenes international commitments that Ethiopia has entered into is not legitimate and cannot be enforced thereby implying being civil servant as a status cannot be a legitimate ground to deprive one running elected government office.

### 5.2. The Ethiopian Electoral, Political Parties Registration and Election's Code of Conduct Proclamation No. 1162/2019

One of the tools that political reformation in Ethiopia was manifested was the reformation of Electoral Commission and election laws. With a view to deliver its promise the Government of PM Abiy has undertaken reformation of critical democracy institutions including reorganization of Election Commission and governing rules. The Government has worked to improve the legal structure and build inclusive governance thereby broadening the playground for participation of political parties.[82] Furthermore, as expressed in the preamble of the Proclamation No. 1162/2019, the reformation aims to ensure an 'all-inclusive,' 'fair and peaceful' participation of all concerned in the electoral process in line with rules of universal and equal suffrage in which citizens can freely express their will in a secret ballot and guarantee a fair, peaceful, free, and democratic election.[83] Further, the Proclamation recognizes the principle of non-discrimination stating: "Any

[79] FDRE Constitution, art. 13(2).
[80] *Id*. art.9(4)
[81] United Nations, 'Vienna Convention on the Law of Treaties 1969' art. 27
[82] Africa News, 'Ethiopian Opposition Parties Reject Electoral Reforms' (*Africanews*, 4 September 2019) <https://www.africanews.com/2019/09/04/ethiopian-opposition-parties-reject-electoral-reforms/> accessed 6 February 2021.
[83] The Ethiopian Electoral, Political Parties Registration and Election's Code of Conduct Proclamation, (n1), see its preamble

Ethiopian whose electoral rights have not been restricted by law or the decision of a court shall be eligible to vote or to be elected... '[84]

However, a cumulative reading of article 5 (1) and 5 (2) of the Proclamation, one can notice that the right to be elected can be restricted when it is provided by law, and it is not discriminatory. Article 30 provides the general eligibility thresholds such as age, residency, mental health capacity, not being legally or judicially restricted, endorsement signature for independent candidates are general candidacy qualifications provided under this proclamation. And article 31of the Proclamation provides additional special criteria for Civil Servant candidates to run for elected government offices. Among others, the Provision requires a civil servant candidate to vacate his/her position as civil servant wit out pay until the election process is complete.[85]

One of the basic principles of the FDRE Constitution is sovereignty of the people that can be manifested through democratic participation which meets the international election standards provided under international human right instruments. Ensuring Universal and equal suffrage that guarantees the right to be elected and the ability to exercise these rights without discrimination for all eligible citizens, as well as the obligation to give equal weight to each vote is one of principles of democratic electoral norms. This is apparently manifested in the preamble of the Proclamation No.1162/2019. Just to reiterate, one of the expressed objectives of the Proclamation was ensuring the participation all concerned thereby applying the principle of universal and equal suffrage in which citizens freely express their will. The Constitution provides only one exception to suffrage right - attainment of the 18 years of age for voter eligibility. Thus, apart from the expressed restrictive conditions, no one can impose either directly or implicitly limitations on principle of universal and equal suffrage. Article 5(2) of the Proclamation 1162/2019 provides the possibility and mechanisms of expression of legitimate restriction. It states: "Any Ethiopian whose electoral rights have not been restricted by law or the decision of a court shall be eligible to vote or to be elected...'.[86] Thus where an express restriction provided by law, and the restriction is justified by reason the categorical restriction cannot be viewed as discriminatory.

---

[84] *Id.* art. 5(2)
[85] *Id*. art.30
[86] The Ethiopian Electoral, Political Parties Registration and Election's Code of Conduct Proclamation (n1), art. 5(2)

With this backdrop it befitting to discuss the implicit deprivation of Ethiopian civil servants to run for elected office. The Ethiopian election law does not expressly exclude civil servants for running to be elected, but simply requires civil servants to leave their office as civil servant and fully engage in the election campaign process. The rationale for this requirement appears to maintain equality of all candidates not use public resources that are not equally available to all candidates. It is true if a civil servant uses vehicles of his/her office, he/she cannot use the vehicle when campaigning while working as a candidate. It is a public property that every candidate is entitled to, that should be available to all competitors. Otherwise, it would undue privilege that can potentially favor one at the expense of all. But what would be if a civil servant resides in the house was granted by the government employer, as a civil servant? Should the civil servant candidate surrender the residential house until the end of election? If negative, what about candidates having no public housing but reside in the rented residence? Is the playground equal and fair to all? It may be argued that a person running to serve the public should equally enjoy public resources. However, it may be unfair to make a civil servant candidate to get out of the residential house that he/she had been living therein as a civil servant. Given the current cost of housing and the difficulty to get or afford for a residential house in Ethiopia, it is not hard to think that surrendering a residential house for the sole reason of running for election is unfair and unthinkable. It is equally unimaginable for a civil servant to run for election if it is required to surrender a residential house that he/she had acquired as a civil servant.

It cannot be generalized that civil servants of other nations would not vacate their office and surrender benefits acquired as civil servant to make the playground of candidacy fair and equal for all contestants. The decision whether to run for election while vacating an office and surrendering or not using publicly provided resources depends upon economic condition of the nation. In jurisdictions that pay high salary or in cheap housing market, weighing the benefits of elected offices or candidacy, a civil servant candidate may not hesitate to run for election while leaving all the benefits of he/she enjoys as civil servant.

How about running for election just by getting leave without pay? Given the current economic condition of Ethiopian civil servants, the pay scale, inflation and overall cost of life that everyone lives from pay cheque to pay cheque (salary to salary) could a civil servant who relies only the earning of his/her employment as civil servant run for election while risking his/her family and

him/herself in danger of hunger for the sake of public service or in expectation of good name or possible fruits of public office? For sure it is unlikely. If Ethiopian civil servants cannot run for election while vacating their office and surrendering the benefits that they have been enjoying on account of their employment position, then what it means to the civil servants? Is it not implicit depravation of their right to serve their nation in elected office? As pinpointed at the outset, this short article attempts to resolve the issue that was ignited by the restrictive provisions of Proclamation No. 1162/2019.

The requirement to vacate public office though apparently justifiable, in effective it is not only restrictive but also prohibitive. As legitimate restrictions should pass the reasonability test, the requirement to vacate civil service offices shall legitimate and reasonable.

In a way of making all contestants election on equal footing, the playground shall be levelled in a way all can equally compete to win the hearts of the public. Thus, negative differential treatment based on any status is prohibited. As indicated elsewhere above, civil servant is a status that cannot be a ground for discrimination. However, non-discrimination does not mean identical treatment. Pierre De Vos (2014),[87] in his book whilst dealing with the right to equality and non-discrimination, stresses that, 'what should be focused on is the impact of the treatment rather than the treatment itself, particularly, group pattern of disadvantage in real context, by analyzing concept of discrimination and unfair discrimination.' In some exceptional cases differential treatment is allowed even required as long as it is reasonable and proportional.

Granting leave for Civil Servant candidates may help prevent conflict of interest and ensure political neutrality, and ensure confidence in the Civil Service, but is it a necessary requirement? As stated by Dawson J (2020),[88] an Australian court rejected a claim of Mr. Phil Cleary noting that, taking leave without pay by a person who holds an office does not change the character of the office that he/she holds, and the person remains the holder of an office notwithstanding that he/ she is not recipient of pay during the period of leave. Receiving payment or not has no relevance for that purpose. So, it is not reasonable to impose such restriction. In addition,

[87] Pierre De Vos, '*South African Constitutional Law in Context'* (University of Cape Town, 2014) Chap.12, 418-465.

[88] 'BarNet Jade - Find Recent Australian Legal Decisions, Judgments, Case Summaries for Legal Professionals (Judgments And Decisions Enhanced)<https://jade.io/article/67724> accessed 27 January 2021

proportionality test requires balance between the legitimate aim pursued and the effects of restriction. Imposing all Civil Servants in general to leave without pay, disregards consideration of the particular circumstances and particular inequalities of social and economic status of those groups violates the principles of proportionality. The restriction has gone beyond what is required to maintain the office's political neutrality, thereby unnecessarily infringes on a fundamental right of civil servants. Therefore, the restriction is unreasonable discrimination incompatible with the constitutional provision article 38 (1) and the State party's obligations under article 25, paragraphs (a) and (b), read in conjunction with article 2, and article 26 of the Covenant and CCPR, General Comment 25, paragraph 16: which clarify that 'measures to avoid any conflicts of interest should not unduly limit the rights protected by paragraph (b) of article 25, ICCPR.'[89]

Further, Proclamation 1162/2019 provides the principle of inclusiveness in its preambles as justification for its amendment "[…] to ensure the participation of every Ethiopian in an all-inclusive[….]'[90] This principle also provides rule which requires that legal recognition of political parties or candidates must not be unreasonably restrictive for political parties and candidates competing in election. It imposes a high level of standard on the state in terms of both negative and positive obligation. As such, any restriction on electoral rights should not exclude some persons or groups of peoples from participating in the political life of the country.[91] In the case at hand, compelling Civil Servants candidates to leave without pay is indirectly excluding civil servants who cannot afford life without pay from the electoral process. As provided in General Comment 25 paragraph 15 of article 25 of ICCPR, "No candidate may suffer any kind of disadvantage due to his candidacy and any excluding legal provision must be justified."[92] As indicated above, article 33 of Proclamation No. 1162/2019 and article 47(2) of the Federal Civil Service Proclamation are not reasonable based on proportionality test.

[89]'CCPR General Comment 25' (n 5) par.16.
[90]The Ethiopian Electoral, Political Parties Registration and Election's Code of Conduct Proclamation, (n13) see preamble.
[91]Maurer and Ardita (n 38) 19
[92]'CCPR General Comment 25' (n 5) par.15

## 5.3. The Implications of Compelling Civil Servants to Take Leave without Pay

As noted earlier, the fact that restrictions on the right to stand for election pursues a legitimate aim does not make the limitation reasonable, if the result of restriction impairs the essence of the right. In addition, considering the social and economic status of those groups or individuals affected by restriction have paramount importance in determining the reasonability of restriction. For example, in financial terms, the Ethiopian Civil Servant is a disadvantaged group with the lowest financial capacity when compared to others. Currently, even the highest salary of a civil servant is hardly enough to sustain the person and his/her family. For instance, according to data collected in 2012 and updated on 20 November 2018 by International Growth Center (IGC) from Ministry of Civil Service, UN Ethiopian Country Office, NGO - CRDA Ethiopia; and Private service provider (Sheraton Hotel), a senior secretary in Ethiopian civil service scale gets two to three times less than a similar secretary in the NGOs or private sector, and 11 times less than one in a donor agency.[93]

In an interview made with member of NEBE Mr. Aman Dawud stated that the restriction could amount to banning civil servants' political participation.[94] Other interviewees, including incumbent candidate Ms. Sa'ada Abduraman, from Prosperity Party stated that criterion incorporated in the Proclamation concerning Civil Servant candidate could affects the right to be elected of Civil Servants.[95] From these observations and analysis of international election standards; compelling civil servant candidate to take leave without pay, at least for more than four months, could be onerous obligation for Civil Servants to exercise their right, thereby impairing the essence of the right to be elected of civil servants which is incompatible with authoritative interpretation of ICCPR, article 25 General Comment 25, paragraph 27 and article 5 of the Covenant.

Moreover, even if the law is equally applied, the ruling party has incomparable economic resources compared to opposition parties. So, it can pay salaries to civil servants who vacate without pay,

---

[93] International Growth Center(IGC, 2018 ), *'A study of the constraints to civil servant productivity in Ethiopia'* available at: < https://www.theigc.org/project/study-constraints-civil-servant-productivity-ethiopia/visited 16 December 2019.

[94]Interview with Aman Dawud, 'An interview made with Mr.Aman Dawud, Office head of Harari Regional state branch office of National Electoral Board of Ethiopia' (26 March 2021).review with Aman Dawud

[95]Interview with Sa`ada Abduraman, 'Interview made with Ms. Sa`ada Abduraman, The head coordinator of Prosperity Party (PP) at East Hararge zone and candidate for HPR' (22 March 2021).

which is not available to the struggling opposition party candidates. In an interview with Mr. Chala Asafa[96] from East Hararge Zone Public Servants' Office, there were about 46,000 Civil Servants in the Zone, but no one took part in candidacy of opposition parties. On the contrary, some civil servant candidates who run for election representing the ruling party did not vacate their civil service position. This shows that forcing civil servants to take unpaid leave in cases where opposition parties are weak, and poor has a negative impact on the recruitment of competent candidates.

## 6. Conclusion

A true democratic election necessitates genuine competition among political party-backed and/or independent candidates, which is enhanced when all eligible citizens participate politically as voters and candidates freely and without unreasonable discrimination. States have the sovereign right to determine how to administer their elections. However, their right is limited through international and regional agreements which set key standards and principles of democratic election such as universal and equal suffrage, secrecy of the vote, the right to vote and to be elected, genuine election, free and fair election, the principle of inclusiveness and the principle of non-discrimination.

Further, it is important to note that the right to be elected in general and the right of civil servants to be elected in particular is not an absolute right and it is subject to limitations in the form of eligibility thresholds that vary between states. The ground of limitations includes incompatibility of office, political neutrality, conflict of interest, and individual capacity. As noted in the article, the existence of these grounds alone does not justify the limitation unless it is reasonable and meets proportionality test. This short work has examined article 33 of Proclamation 1162/2019 which compels civil servants in Ethiopia to leave without pay if they wish to participate in an election as candidates. It has shown that though the law pursues a legitimate aim of maintaining political neutrality, the means used is unnecessary and disproportional as it imposes a significant burden on the right to be elected of civil servants in Ethiopia. As such, it is incompatible with the FDRE Constitution and international human rights treaties that Ethiopia has ratified. Accordingly, the article underscores the importance of amending this provision in a manner that conforms to the

[96] Interview with Chala Asafa, 'An interview made with Mr. Chala Asafa, Coordinator of Human Resource Management at Oromia Public Servant Bureau; East Hararge Public Servant Office.' (26 March 2021).

Constitution and international human rights standards applicable to Ethiopia. The amendment should provide two options: grant leave with pay that accompanied by reasonable requirement of sizable number of endorsement signatures for candidate registration; to avoid flood of civil servants contestants without hope of success and waste public resources or inimical to public service. Moreover, the article recommends avoiding general restriction by categorizing civil servants in groups considering sensitivity of their office to politics and possibility of conflict of interest, level of participation, and their financial capacity. As such, they may be grouped as politically restricted group, politically unrestricted but situation based and politically free group.

# The Notion of 'Business': An activity? A responsibility? An entity? Or A property? (Reflection on Issues for Consideration)

**Lantera Nadew***

## I. Perplexities Involving Use of the Term 'Business'

We often use the term 'business' in our daily interactions in various contexts. It is not uncommon to notice one saying: "It is none of my business," or "My family business is doing good," "Sale of garage business," or "Let's do business," and so forth. Ordinarily, it is common to use the term business in the sense of activity, responsibility, or entity. When one says, "it is none of my business," we imagine absence of responsibility or when one says, "it is a profitable business, or the business is not good," it implies a transaction or venture. In the expression 'business organization,' the term business denotes entity. In the sense of Comm. Code (Both in 1960 and 2021), the notion of 'business' applied in the sense alien to the popular use of the term. As defined in the Comm. Code, the notion of business is neither a responsibility nor an activity, or transaction. In a day-to-day usage, the notion of business is very familiar, but understood in different contexts. The legislative definition as expressed in the Comm. Code of 2021 is not simple enough to capture.[1] It is, therefore, fair to question what business is and how it works in real life.

This short note aims to shed light on the nature and constituent elements of the notion of "business." The reflection is believed to provoke professionals in the field for further illumination of the notion of business and its legal effects. Varied usage of the term business is also reflected in formal use of the term in non-business legislations, which define the term business as an activity.[2] This view aligns with the dictionary meaning of the term. The professional law

*LL.B., LL.M., SJD, Assistant Professor, School of Law and Federalism, ECSU. The reflection is a modified version of a draft version of the book on Ethiopian Law of Traders and Business Organizations.

[1] The Comm. Code defines the term business technically which is different from the popular sense of the term.

[2] See for instance, Art. 2(2) (a) of the Federal Income Tax Proclamation, defines the term business as, "any industrial, commercial, professional, or vocational activity conducted for profit and whether conducted

dictionary illustrates the notion of "business" as, "Employment, occupation, profession, or commercial activity engaged in for gain or livelihood."[3] The legislative definition of the term as envisaged both in the Commercial Code of 1960 and the revised version (Commercial Code of 2021) business may ridicule non-lawyers or even puzzle beginners of law. The Commercial Code of 2021 defines the term business as an incorporeal chattel.[4] This further fuels the complexity. At first confrontation with Art. 124 of the Comm. Code of 1960, or Art. 106 of the Commercial Code of 2021, it may not surprise if a reader screams "what!" The definitional provision necessarily appears calling for a definition. Use of the terms like 'incorporeal chattel,' 'intangible movable,' 'property brought together and organized for the purpose of carrying commercial activity' is an uphill battle to master. What is incorporeal chattel? How business an intangible property moves? What is the relationship between business as an intangible property and tangible properties that are brough together and organized? A brief analysis of the nature of business in sense of the Comm. Code will answer these issues.

In the words of the Code, the term business is, "[…] an incorporeal movable consisting of all movable properties brought together and organized for the purposes of carrying out any of the commercial activities specified in Article 5 of this Code."[5] In legislative perspectives therefore the term "business" is defined as a property – an invisible property – a property one cannot see but can enjoy its pecuniary effects. In the property sense of the term, "business" is akin to other tangible properties, can be sold, donated or bequeathed, or can be transferred from one person to the other.[6] The Code's definition of the term business as an intangible property is far away from the popular sense of the term.[7] Is business really a property? Further, no wonder even one questions the property nature of an intangible movable. Though the property nature of invisible

---

continuously or short-term, but does not include the rendering of service as an employee or the rental of buildings." Federal Income Tax Proclamation, Proc. No. 979/2016, *Neg. Gaz.*22nd year 104, Art. 2(2)(a).

3 Black's Law Dictionary Six Edition

4 Comm. Code of Ethiopia, Proc. No. 166, 1960 NEG. GAZ. 19th Year No. 3 A.A. ( Herein after Comm. Code of 1960) Art. 124. Almost the same wordings used in Art. 106 of the Comm. Code of 2021, which avoided the term "chattel" to movable. This change avoids confusion of non-lawyers. Ordinary use of a term is preferred to technical meaning.

5 Comm. Code of Ethiopia, Proc. No. 1243/2021, Fed. NEG. GAZ. Extra Ord. Issue Year 27 No. 23 A.A. April 2021 (herein after Comm. Code of 2021). Art. 106; Comm. Code of 1960. Art. 124.

6 JOHN G. SPRNKLING *ET AL*, GLOBAL ISSUES IN PROPERTY LAW, 1(Thomson West, 2006)

7 Comm. Code of 2021. Art. 106.

property is hard to understand to some, the law considers an intangible property as a property and bestows legal protection.

A critical look at the elements of the legislative definition of the term business ignites further issues. The extent of corporeal chattel that the notion of business includes, the modalities of transacting business, how ownership of business may be proved, who may own a business, and so forth. Could non-traders or non-commercial business own a business? Both provisions (Art. 106 of the Comm. Code of 2021 and its predecessor, Art. 124 of the Comm. Code of 1960) define the notion of business, as a property that emerges out of *commercial activity* (any one or more the activities enumerated in Art. 5 of the Comm. Code). Literal understanding of Art. 106 reveals that only traders and commercial business organizations can operate business. A trader, in the sense of the Commercial Code, is a person who carries out anyone or more of the activities enumerated in Art. 5 professionally and for gain.[8] By implication therefore non-traders[9] do not operate business.

Similarly, in old days, the same rule applied to non-commercial business organizations.[10] In accordance with Art. 10 of the Comm. Code of 1960, business organizations, depending upon the activity they carried on, are categorized into commercial or non-commercial business organization. Before the coming into force of the Comm. Code of 2021, if a business organization carried out anyone or more of the activities enumerated in Art. 5 of the Comm. Code, it was classifieded as commercial business organization. However, companies (share company and private limited company),[11] irrespective of the activity they operate, were considered as commercial. There was

---

8 Comm. Code of 2021. Art. 5.

9 Non-trader does not always mean persons operating non-profit activity. It includes all persons who are not engaged in any one or more activities enumerated in Art. 5 of the Comm. Code Art. 5 of the Comm. Code enumerated almost all activities that make persons engaged in traders. Small scale workers and handicraftsmen, even if they operate anyone of the activities stated in Arti. 5 of the Comm. Code. Generally, non-trader status includes any activity other than those enumerated in Art. 5. Thus, person that can possibly own business are limited; see also Art. 107(10 of the Comm. Code of 2021 which states, "Every trader operates a business." By implication non-traders cannot operate business.

10 The Comm. Code of 2021 has no provision analogues to Art. 10 of the Comm. Code of 2021. Therefore, in silence of the Code, and other legislations that do not make any distinction between commercial and non-commercial business organizations, it is doubtful to assume classing business organizations as commercial and non-commercial still works. The policy rationale behind classing as commercial or non-commercial was to distinguish organization that may be relived from certain defined obligations. But now all business organizations are required to discharge those obligations. Currently, all business organizations have the obligation to be registered, keep books and accounts, and should get business license. Therefore, in effect, there is no difference between commercial and non-commercial business organizations.

11 The Comm. Code of 1960 recognized only two forms of companies.

no non-commercial company. Other business organizations (other than ordinary partnership),[12] depending upon the activity they carried out, were classed as commercial or non-commercial.[13]

In accordance with Art. 10 of the Comm. Code of 1960, a business organization may be branded as commercial either if it carried out any one or more of the activities enumerated in Art. 5 or based on the nature of business organization. Companies, irrespective of the activity they carry on, were always regarded as commercial business organization. Other business organizations (partnership and joint venture) can only be viewed as commercial business organizations if and only if they carry out commercial activities as enumerated in Art. 5.[14] There is no analogous provision in the Comm. Code of 2021. Does it mean there is no classification as commercial and non-commercial business organizations in the Comm. Code of 2021? Doubtful. The silence of the Comm. Code of 2021 has further complicated setting boundary of business organizations that may operate business. If the Commercial Code of 2021 has avoided commercial or non-commercial classification of business organizations then why it uses the old technical terms like: 'commercial activities, trade' etc? If the silence and other legislations have changed the rule by making categorization of business organizations as commercial and non-commercial in effect meaningless, then one can conclude that all business organizations can own and operate business. It also appears possible to pose the same argument in respect to non-trader businesspersons. Leaving the issue of persons or organizations that may own business, unresolved, let's deal the issue of actual meaning of business and its elements as defined in the Comm Code.

## II. What is Business Actually?

In the sense expressed in the Commercial Code of 2021, the term "business" is mainly an incorporeal chattel. It is an intangible property that emerges out when one (a businessperson) operates a commercial (business) activity. It is a value that can be created by the operation of commercial activity. If the operator carries the business skillfully and attracts more customers, the

[12] The Comm. Code of 2021 has scrapped the ordinary partnership from Ethiopian business organization. Now on wards, in Ethiopia there no partnership captioned as ordinary partnership can be set up.

[13] Art. 10 cum 213 of the Comm. Code of 1960.

[14] Commercial activities are list in Art. 5 of both the Comm. Code of 1960 and Comm. Code of 2021. The enumeration of Art. 5 of the Comm. Code of 2021 is very extensive while the listing of Art. 5 of the Comm. Code of 1960 is fairly short.

value of the business increases. Conversely, if the operator is not doing well, the business would attract less number of customers. In this case, the money value of business would be very small. Despite variation of value, all traders and business organizations have business of some sort. By implication thus total absence of business means the person or organization has stopped the business activity. If no customer shows up or no one wishes to transact with a given trader or business organization, then it is assumed that the trader or business organization will be forced to close and stop what he/she has been attempting to do. This is not a scenario likely to happen in cases and circumstances. Though a trader or business organization may experience slow traffic of customers, some may wish to transact with a businessperson. There may be price negotiation or quality specification that may not be profitable to the expected level, but possibly, some limited number of customers would be willing to maintain business relationship. In this case therefore the businessperson has business of some value.

Though the money value of businesses of all traders or business organization is not identical, all businesses have a certain value, which depends upon the quality of service rendered or the significance of items produced or offered for sale. A trader or business organization may be wealthy if the services or products are highly demanded or more customers are willing to deal or maintain business relationship with the trader or business organization. With a view to win market competition and attract more clients a trader or business organization may endeavor, by investing more resources and labour, to hire competent personnel that can offer good customer care. The value of business that may emerge from a huge investment will be higher as long as it is the right kind of investment. Being a product of labour and investment, like any tangible asset, business is a property that can be transacted. It can be sold,[15] leased,[16]mortgaged,[17] or contributed to business organizations.[18]

However, in traditional societies, it may be hard to cognize the property nature of an inviable asset. How can one value a property that cannot be seen or touched? Ordinarily, it is a challenge to perceive and value a property 'without a body or substance.' Even the owner of a business may

[15] Comm. Code of 2021. Art. 122
[16] *Id*. Art. 116
[17] *Id*. Art. 143
[18] *Id*. Art. 168.

not understand the level of his/her intangible wealth. Intangible property is a property "[w]ithout body or substance; in a material nature …" and incorporeal movable (chattel) is "a class of incorporeal rights growing out of or incident to things personal, such as: patent-rights and copyrights."[19]

The notion of "business" is substantially an incorporeal chattel, but it also holds some corporeal chattels that the trader or business organization uses when running the activity. The Commercial Code of 2021 points out the possibility of inclusion of movable properties under business stating that "a business may consist of corporeal elements such as equipment or goods."[20] This is a restatement of what is already provided in the definitional provision.[21] A tangible property to be considered as a component of business should be destined to operate the business activity. A businessperson or business organization may use variety of movable properties in business operation. Movable properties like vehicles, machines, computers, printers, scanners, phones, furniture and fixtures, or other office equipment that the trader uses while operating his/her venture are parts of business. The inclusion of corporeal chattel in business is not a necessary requirement. In some very limited circumstances, a person may carry out trade without using one or more movable properties. A broker, for instance, may not have an office or a vehicle destined to operate a business, but, if considered as a trader, he/she owns a business of some value. In this highly digitalized economy, it is not surprising if one works simply using his/her cellphone at his/her living room, or his/her own or even family car in getting contact with customers. A locksmith, for instance, can put all his locksmithing stuff in the trunk of his family car waiting for call. Whenever called he/she may move using his personal car. He/she doesn't need to have a permanent business place, or even he/she may not use the same car permanently.[22] As personal property does not makeup business or a living room sofa set is not business property that can constitute business. However, in normal course of things, one cannot imagine a business activity or a trade of some sort without being assisted by a property.

As it is clearly provided in Article 106 of the Commercial Code of 2021, only movable properties

---

19 *Id.*

20 Comm. Code of 2021, Art. 110.

21 Art. 106 of the Comm. Code of 2021.

22 Such small-scale workers however not captioned as traders. Therefore, it is possible to argue that such small-scale workers and handicraftsmen/women do not have business to build or sell.

used for commercial activity can make up business. The expression, "[…] consisting of all movable property brought together and organized for the purpose of carrying out any of the commercial activities [….]"[23] proves the fact that immovable property does not constitute business. The express statement stating that only movable properties can make up business avoids confusions, but even in absence of this expression, the nature of the term business itself indicates that only movable properties can be part of business. A business is a movable property; hence, it is awkward to talk about a movable property consisting of an immobile property. Thus, a building that a trader or a business organization carries out a commercial activity does not constitute business.

The other possible confusion is the use of the term business in Amharic. The Amharic version of the Commercial Code of 2021, as well as its predecessor, the Commercial Code of 1960, use the expressions " የንግድ ሙደብር" to mean "business." It sounds like a place where a trader carries out his/her commercial activity. Is a store or shop where a trader carries out commercial activity an intangible property? What if a trader does not have a settled place of business? Certain traders, depending upon the nature of the activity, may not necessarily settle at a given place. During registration of the business the trader may simply provide his residential location and run business moving here and there or whenever called by his/her truck that carries all stuff needed for the business activity. Can we designate the trader's residential location as a business? It is true the truck, being a corporeal chattel, is a component of business. Hence, a trader on account of the nature of trade carried out, may not have a definite business place but can provide his/her residential address in the commercial register. Can we say such "traders" do not have business? The answer is quite clear; No! Is connoting the expression, " የንግድ መደብር" as business proper use of the term? If not what is the possible counterpart of the term "business?" Or else can we consider the terms, "የንግድ መደብር" as a technical Amharic counterpart of the term "business"? [24]

[23] Comm. Code of 2021. Art. 106.

[24] Assessing legislative meaning, or legal jargons is not the theme of this work but understanding of the true nature of legal expressions will facilitate or our perception and application of the law.

## III. Business is Mainly Goodwill

In addition to the corporeal chattel that the notion of business may comprise, the Comm. Code of 2021,[25] specifically enumerates some of the incorporeal chattels that constitute business.[26] As provided in Art. 109(1) of the Comm. Code of 2021, the main constituent element of business is goodwill. Goodwill is an important element of business. It is, therefore, crucial to explore the meaning and nature of 'business.' But comprehension of an exact nature of the term, "goodwill" is also an uphill journey. What actually "goodwill" is and how can we perceive its property nature or gauge its economic value? We often hear about "goodwill" and have our own sense of understating of the term, but it may be a painstaking attempt to define the expression goodwill precisely or explain its exact nature. Article 112 of the Commercial Code of 2021 defines the term "goodwill" on the basis of its source and its pecuniary effects. It illustrates "goodwill" in terms of its creation as follows:

> The goodwill results from the creation and operation of a business and is of a value which may vary according to the probable or possible relations between a trader and third parties who may require from him goods or services.[27]

The Commercial Code of 2021 is substantially identical with it is predecessor, the Commercial Code of 1960, but it goes beyond a sheer source of goodwill. In accordance with the Commercial Code of 2021, "goodwill" is a value created by (resulted from) commercial activity, and its value advances as a result of the attitude of customers toward goods and services offered by the trader.[28]

The Commercial Code of 2021 does not plausibly define the term "goodwill," but it apparently illustrates how goodwill emerges out in commercial activities. The apparent definition is cloudy that demand explanatory work. The Codes describes goodwill in terms of value, and the value created by the attitude of customers toward commercial activity of trader. How can we measure

---

25 *Id*, Art. 109.
26 *Id*.
27 Comm. Code of 2021. Art. 112.
28 As the English version of the Code is not publicly available, this is author's translation from the Amharic version of the Comm. Code of 2021.

the attitude of customers in terms of money? Is it possible to gauge the money value of attitude?

As briefly highlighted above, whenever a trader operates any one or more of the activities stated in Article 5 of the Commercial Code,[29] a property known as "business" emerges thereby yielding an intangible property called 'goodwill'. Therefore, every trader or business organization operates business, which can be expressed in terms of goodwill. To 'produce' goodwill the creation of business organization or registration of a trader in the commercial register or getting a business license is not sufficient: in order for a venture to generate goodwill, the business activity should be operational. The pecuniary value of goodwill depends upon the quality of operation of business activity. If the trader or business organization offers quality products or services that best satisfy the interest of customers, more customers would stay in hold with the trader or business organization. A satisfied customer will obviously decide to keep business relationship with the trader. That is why the Commercial Code tries to define the expression "goodwill" in terms of customers' behavior.[30] The attitude of customers may vary depending upon the level of satisfaction, quality of goods and services offered. Accordingly, Comm. Codes (both 1960 and 2021) guage the value of goodwill in terms of probable and possible relationship between the trader and customers.[31] If the business of the trader attracts more customers who have decided to continue commercial relationship with the trader, the value of goodwill is expected to be high. On the contrary, if the quality of goods and services offered by the trader is poor, the trader still has business and goodwill but the economic value of business and its fruit – goodwill – is very minimal. It will eventually grow up should the trader makes effort to boost up the quality of business activity by rendering attractive services, customer care, and applies market tools including advertisement.

The Amharic counterpart of the term 'goodwill' as provided in the Comm. Code of 1960 was very intriguing. It captioned the expression "goodwill" as, 'ደንበኛ ገበያተኛ'.[32] At first glance one may be ridiculed. Why the legislature of 1960 opted to mean goodwill 'ደንበኛ ገበያተኛ'? No legislative explanation was provided, and no rationale is available. The only possible remedy to cognize

[29] Art. 5 of Comm. Code of 2021 defines the term "trader."
[30] Comm. Code of 2021, Art. 112.
[31] *Id.*
[32] Comm. Code of 1960. Art. 130.

goodwill was to resort to the English term and experiences of other jurisdictions. Literally the term 'ደንበኛ' may be understood in two contexts. The most relevant context is customer. First, the most common context relevant to 'goodwill' is customer, and the term 'ገበያተኛ' literally means marketer. Both Amharic terms 'ደንበኛ ገበያተኛ' literally mean a real or true marketer. This meaning has nothing to do with the meaning of the term' goodwill'. The Comm. Code of 2021 has changed this expression by coming with the expression, *'መልካም ስም '*.[33] But the Codes does not reveal how "መልካም ስም" (goodwill) may be valued.

The perplexity of defining the term business extends to its main constituent element -- "goodwill." Supposedly, the elusiveness of the term had forced the legislature of the Comm. Code of 1960 simply to illustrate how goodwill emerges out rather than what goodwill actually was. To illustrate the notion of "goodwill" means indicating how *business* emerges out. The Amharic term, 'መልካም ስም, ' appears relatively better, but still blurry. The terms, *'መልካም ስም '* is equivalent to the word 'reputation, ' or 'good name". Is the notion of 'goodwill' really equivalent to reputation or good name? Doubtful. It is apparently true that 'good name' or 'reputation' is weighed in terms attitude of customers. Customers would like to continue business relationship with the trader or business organization if the products or services rendered is satisfactory. The satisfaction obviously generates "good name" or "good reputation," to the trader or business organization. In this regard, the expression, "መልካም ስም" is more expressive, and mitigates the potential confusion. It would be more effective if the Comm. Code delineates the contours of the term goodwill clearly.

The problem of defining goodwill is not peculiar to Ethiopia. It is a global hassle. Jurists have been battling to find out a working meaning of the notion of goodwill. English judges took forefront in the battle of the defining the term goodwill. Lord Eldon describes goodwill as, "… nothing more than the probability that the old customer will resort to old place."[34] Thus, if an old customer craves to maintain unbreakable business bondage with a given trader or business organization, judges suppose the tendency of the customers as the expression of goodwill. The monetary value of goodwill is so great if customers of a trader decide to keep everlasting business relationship with

[33] Comm. Code of 2021. Art. 112.

[34] Lord Eldon defined the goodwill when disposing an English case *cruel well v Lye*. The case was reported in (Cruel *well v Lye* 17 vest 335).

the trader. On the contrary, if old customers look for alternative option for the same service or goods, the value of the goodwill is minimal. In this regard, the notion of goodwill may be described in terms of customers' behavior. According to Lord Machaghten, goodwill is:

> …the very sap and life of the business, without which the business would, yield little or no profit. It is the whole advantage whatever it may be of the reputation and connection of firm, which may have been built up by years of honest work or gained by lavish expenditure of money.[35]

Hence, the terms "business" and "goodwill" are highly intertwined. Therefore, if there is no goodwill, one cannot expect the existence of business or commercial activity. In other words, if no one dares to transact with the trader, there will be no goodwill. This in turn means there is no business and the trader would abandon the commercial activity. However, if few people or very few customers are willing to transact with a given trader, there is still goodwill and business, but its economic value is minimal. Unless the trader does some improvement or takes a corrective action to boost up the quality of service or products, the value of the goodwill will diminish eventually. Lord Machaghten was right in gauging goodwill in terms of the whole advantage that a trader enjoys as a result of his/her commercial activity.[36]

In addition to goodwill, the notion of business holds other constitutive elements that the law confers on traders. Article 109 of the Commercial Code of 2021 enumerates additional invisible rights that a trader may own as a result of the business activity he/she runs.[37] Additional constituent elements of business includes: trade name, trademark, the right to lease premises, patent, or copyright.[38] These expressions are self-explanatory and do not call for further analyses in this short commentary.

---

35 Lord Machaghten in the case, *Trego v Hunt* (*Trego v Hunt* (1896) AC 7, 16)

36 *Id.*

37 Art. 109 of the Comm. Code of 2021 enumerates additional elements that make up business.

38 The Comm. Code of 2021 has referred trade name, trademark, and patent to specific laws that set forth rules governing each of them. Comm. Code of 2021, Art. 115.

## IV. Conclusion

This short reflection aimed to expose possible issues that may arise from the notion of business as expressed in the Ethiopian Commercial Code. The work is not deep enough but believed to provoke professionals in the field to make further research. Until a detailed research and analysis is made, the short expository work can help law students, the academia and the judiciary solve possible issues that may arise in cognizing the terms, especially in issues involving goodwill and unfair competition.

The term 'business' is very important in commercial activity, but it is presented in the Commercial Code in very technical and vague terms. Business is a very critical invisible property that emerges out from commercial activity. The notion of business may appear to goodwill, but the two expressions are not exactly same. The term 'business' holds additional elements, like corporeal chattel used by trader or by business organization while operating business activity. Business also includes other intangible properties like copyright, trademark, tradename, patent, and the right to lease premises. Business, though an invisible property, it is a property that can be transacted like any other asset. Business may be sold, leased, mortgaged, or subjected to usufruct.

Additionally, it is better if proper nomenclature of the new Commercial Code is used when cited for the first time, i.e., Commercial Code of Ethiopia Proclamation No. 1243/2021. It is okay if you use "Commercial Code of 2021" after first using the proper nomenclature.

## Case Comment

### የፍቺ ውሳኔ የጋብቻ ውልን ቀሪ ያደርጋል ወይስ ኢያደርግም?

**በዶ/ር ደጀኔ ግርማ ጃንካ**
**በኢትዮጵያ ሲቪል ሰርቪስ ዩኒቨርሲቲ የህግ መምህር**
**ጠበቃና የህግ አማካሪ**

በኢትዮጵያ ውስጥ አሁን ባለው ሁኔታ ህጋዊ ጋብቻ ሁለት ተቃራኒ ፆታ ባላቸው ሰዎች መካከል ሊፈፀም የሚችል ግንኙነት ወይም ድርጊት መሆኑ የሚታወቅ ነው።[1] ይህ ግኙነት በፅሁፍ ውል መመስረት ያለበት እና በአራት ምስክሮች ማለትም ሁለት ከባል እና ሁለት ከሚስት በኩል መረጋገጥ ያለበት ውል እንደሆነ ግልፅ ነው።[2] በዚህ ውል መሰረት ተጋቢዎች የጋብቻ/የትዳር ግንኙነት በመካከላቸው ሲመሰርቱ ቀሪውን የህይወት ዘመናቸውን አብሮ በፍቅር፣ በመከባበር፣ መተጋጋዝ፣ እና በመረዳዳት ለማሳልለፍ በመወሰን ነው።[3] በዚሁ መሰረት ሰዎች ወደ ጋብቻ ይጋባሉ፤ ትዳር ይመሰርታሉ፣ ከትዳር አጋሮቻቸው ጋር እስከ መጨረሻም ይኖራሉ። ነገር ግን በተለየዩ ምክንያቶች የታሰበው ሳይሆን ወደ ጋብቻ ከሚገቡ ሰዎች መካከ የተወሰኑቱ ጋብቻቸው ሊፈርስ ይችላል። ከእነዚህ ምክንያቶች መካከከል አንዱ ፍቺ ነው። ፍቺ በፍርድ ቤት የሚሰጥ ውሳኔ ሲሆን ይህ ውሳኔ በተጋቢዎች መካከል የነበረው ግንኙነት የሚያቋርጥ ነው። ከዚህ ጋር ተያይዞ በርካታ ነጥቦች ሊነሱ ቢችሉም የዚህ ፅሁፍ ትኩረት አንዱ ላይ ብቻ ሲሆን እርሱም *ሰዎች የፅሁፍ የጋብቻ ውል ፈፅሞ ከተጋቡ በኋላ ጋብቻቸው በፍ/ቤት ቢፈርስ የፍቺ ውሳኔ በጋብቻ ውል ላይ ያለው ውጤት ምንድን ነው?* የሚል ነው። ለዚህ ጥያቄ መንስዔ የሆነ አንድ የፍ/ቤት ውሳኔ ሲሆን የነገሩ አመጣጥ በአጭሩ እንደሚከተለው ነው።

ከሳሽ አቶ "ሀ" በፌደራል የመጀመሪያ ደረጃ ፍ/ቤት የካ ምድብ ፍ/ብሄር ችሎት በኮ/መ/ቁ 128733 በተከሳሽ ወ/ሮ "ለ" ላይ በ19/11/2009 ዓ.ም የውል ይፍረስ ክስ ያቀረበ ሲሆን ክሱም "እኔና ተከሳሽ በ07/06/2007 ዓ.ም. ለመጋባት የፈረምነው የጋብቻ ውል የተፈረመው በተከሳሽ ተንኮልና ማታልል ስለሆነ ይህ የጋብቻ ውል ይፍረስልኝ፣ ህጋዊ ውጤት የለውም ይባልልኝ" የሚል ነው።[4] ተከሳሽ ወ/ሮ "ለ" በበኩላቸው የቀረበባቸውን ክስ የተቃወሙት ሲሆን መቃወሚያውም "እኔ እና ተከሳሽ ተዋድደን እና ተፋቃቅረን ያለአንዳች ጫና የሃገር ሽማግሌዎችና የሃይማኖት አባቶች ባሉበት ቦታ በ07/06/2007 ዓ.ም. ትዳር ለመመስረት የጋብቻ ውል የፈረምን ቢሆንም በመካከላቸው በተፈጠረው ችግር ምክንያት ይህ ውል ፈርሶ ጋብቻችን ቀሪ እንዲሆን በፌደራል የመጀመሪያ ደረጃ ፍ/ቤት 5ኛ ፍ/ብሄር ችሎት በመ/ቁ 122235 በቀን በ22/07/2009 ዓ.ም. ተወስነዋል፤ በአንድ ችሎት የፈረሰ ውል ደግሞ እንደገና በሌላ ችሎት እንዲፈርስ ጥያቄ ሊነሳበት ስለማይችል ወይም አንድ ጊዜ የፈረሰ ውል እንደገና ይፍረስ የሚል ክስ ሊቀርብ ስለማይችል አሁን የቀረበብኝ ክስ የክስ ምክንያት (cause of action) የለውም ተብሎ በፍ/ስ/ስ/ህግ አንቀፅ 33(2) መሰረት ውድቅ መደረግ አለበት" የሚል ነበር።[5]

---

[1] *ተመሳሳይ ፆታ ያላቸው ሰዎች እንዲህ ዓይነት ግንኙነት ሊፈጥ አይችሉም፤ ምክንያቱም በወንጀል ህጉ አንቀፅ 629 መሰረት የተከለከለ ነው።*

[2] *ለምሳሌ የተሸሻለውን የቤተሰብ ህግ አንቀፅ 44ን እና የኦሮሚያ የቤተሰብ ህግ አንቀፅ 60ን ይመልከቱ።*

[3] *የተሸሻለው የቤተሰብ ህግ አንቀፅ 49 ባል እና ሚስት አርስ በእርሳቸው መከባበር፣ መተጋጋዝ፣ እና መረዳዳት እንዳለባቸው ይደነግጋል። የኦሮሚያ የቤተሰብ ህግ አንቀፅ 65(2) ተመሳሳይ ድንጋጌ ይዘዋል።*

[4] *የክሱን ሙሉ መረጃ በፌደራል የመጀመሪያ ደረጃ ፍ/ቤት የካ ምድብ ፍ/ብሄር ችሎት ከኮ/መ/ቁ 128733 መመልከት ይቻላል።*

[5] *የመልሱን ሙሉ መረጃ በፌደራል የመጀመሪያ ደረጃ ፍ/ቤት የካ ምድብ 5ኛ ፍ/ብሄር ችሎት በመ/ቁ 122235 መመልከት ይቻላል። ይህ ጉዳይ ተከሳሽ ባቀረቡት መቃወሚያ መሰረት ባይሆንም እስከ ሰበር ሰሚ ችሎት ድረስ ሄዶ የከሳሽ ክስ ውድቅ ተደርጓል፤ በዚህ ምክንያት ተከራካሪዎች ወገኖች በመጨረሻ ላይ ባደረጉት ስምምነት መሰረት የንብረት ክፍፍል ተፈፅሟል።*

ይህ አጭር ፅሁፍ ለመዳሰስ ከሚያስበው ነጥብ አንፃር የነበረው ታሪክ ከላይ የተጠቀሰው ሲሆን ክስ የቀረበለት ችሎት ከላይ የተገለፀውን የተከሳሽ መቃወሚያ አልፎታል ወይም ውድቅ አድርጎታል፡፡ ይህ መቃወሚያ ውድቅ የተደረገው እንደ አዲስ ይፍረስ ተብሎ ክስ የቀረበበት ውል ቀድሞውኑ በሌላ ችሎት ለፍቺ ጥያቄ መሰረት ሆኖ ክስ ቀርቦበት ጉዳዩን የያዘው የቤተሰብ ችሎት ውሉን አፍርሶ ጋብቻው በፍቺ ቀሪ እንዲሆን እንደወሰነ እየታወቀ ነበር፡፡ እንዲህ ዓይነቱ አካሄድ *በውል መሰረት የተፈፀመ ጋብቻ ቀሪ እንዲሆን የፍቺ ውሳኔ ከተሰጠ በኋላ ውሉ ለብቻው ፀንቶ የሚቆይበትን አግባብ አለ ወይ?* የሚል ጥያቄ የሚያስነሳ ይሆናል፡፡ የፍቺ ውሳኔ ሰዎች ትዳር የመሰረቱበትን ቃል-ኪዳን (ውል) መፍረስ የማያስከትል ከሆነ እንዴት ግንኙነት ሊያቋርጥ ይችላል? ተጋቢዎቹን አንድ ላይ አስሮ ባል እና ሚስት ያደረጋቸው ውሉ አይደለም ወይ? ተጋቢዎቹ በፍ/ቤት ውሳኔ መሰረት ተለያዩ ማለት አንድ ላይ ያስተሳሰራቸው ወል (ህግ)[6] ቀሪ ሆነ (ተሻረ) ማለት አይደለም ወይ? ውሉ ፍቺ በሚወሰንበት ጊዜ ቀሪ ከሆነ ደግሞ በሌላ ችሎት ውሉ ይፍረስልኝ የሚል ጥያቄ ሊቀርብ ይችላል ወይ? እነዚህ ጥያቄዎች መልስ የሚፈልጉ ናቸው፡፡ በመጀመሪያ እይታ ቀላል ሊመስሉ የሚችሉ ነገር ግን በተግባር ከፌደራል የመጀመሪያ ደረጀ ፍ/ቤት እስከ ሰበር ሰሚ ችሎት ድረስ የደረሰ ክርክርን ያስከተሉ ነበሩ፡፡

ተጋቢዎች ሁለት ዓይነት ውሎችን ሊፈፅሙ የሚችሉ ሲሆን ውሎቹም ጋብቻ የሚያቋቁሙበት ውል (የጋብቻ ውል) እና የንብረት ግንኙነቶቻቸውን የሚቆጣጠሩበት ውል ናቸው፡፡ ከላይ የተገለፀው እና ከሳሽ እንዲፈርስለት የጠየቀው ውል በከሳሽ እና በተከሳሽ መካከል የሚኖረውን የንብረት ግንኙነት ለመቆጣጠር የተፈፀመ ራሱን የተለየ ውል አይደለም፡፡ ከሳሽ እንዲፈርስለት የጠየቀው ውል ጋብቻው እራሱ የተመሰረተበት ውል ነው፡፡ በመሆኑን በሁለቱ ወገኖች መካከል የነበረው ውል አንድ ብቻ ነበር፡፡ የፍቺ ውሳኔ እንዲሰጥ ከሳሽ ጥያቄ አቅርቦ የነበረው ከሳሽ እራሱ ሲሆን የፍቺ ማመልከቻውን ለፍ/ቤት ሲያቀርብ ይሄንኑ ውል እንደ ማስረጃ በማያያዝ ነበር፤ የፍቺ ውሳኔውም በዚሁ ውል መሰረት በሁለቱ ወገኖች መካከል የትዳር ግንኙነት የነበረ መሆኑ ከተረጋገጠ በኋላ የተሰጠ ነበር፡፡

የሆነው ሆኖ ትዳር (ጋብቻ) የተመሰረተው በውሉ መሰረት እስከሆነ ድረስ ጋብቻው ቀሪ ሊሆን የሚችለው ሰዎቹን ያስተሳሰረው ቃል-ኪዳን ወይም ውል ቀሪ ሲሆን ብቻ ነው፡፡ ውሉ ቀሪ ካልሆነ በውሉ መሰረት የተመሰረተው ግንኙነት ቀሪ ሊሆን አይችልም፤ ሁለቱ የአንድ ሳንቲም ሁለት ገፅታዎች ናቸው፡፡ በተጨማሪ የጋብቻ ውል ቀሪ የሚሆነው (ውጤት ማመንጨት የሚያቆመው) በውሉ ውስጥ የተካተቱ ሁሉንም ጉዳዮች በሚመለከት ነው እንጂ በከፍል የተጋቢዎችን የግል ግንኙነት በሚመለከት ብቻ ሊሆን አይችልም፡፡ በፍቺ ውሳኔ መሰረት ቀሪ የሆነ ውል በተጋቢዎች መካከል ያለውን የባልና የሚስት ሁኔታን ብቻ ቀሪ አድርጎ ሌሎች ጎዳዮችን በሚመለከት ፀንቶ ሊቀጥል አይችልም፡፡ የፍቺ ውሳኔ የጋብቻውን ውሉ እስከነሙሉ ይዘቱ ቀሪ የሚያደርግ ነው እንጂ የተጋቢዎችን የግል ግንኙነት በማቋረጥ ላይ ብቻ የሚገደብ አይደለም፡፡

ከላይ ከተሰጠው ማብራሪያ አንፃሪ ሲታይ በፍቺ ውሳኔ መሰረት ቀሪ የሆነ ውል እንዳልፈረሰ ተቆጥሮ ውሉ ይፍረስ የሚል አዲስ ክስ እንደገና የሚቀርብበት አግባብ አይኖርም፡፡ እንዲህ ዓይነት ክስ የሚቀርብ ከሆነ ክሱ መንስዔ ወይም የክስ ምክንያት (cause of action) ስለማይኖረው በፍ/ስ/ስ/ህግ አንቀፅ 33(2) መሰረት መቃወሚያ ከቀረበበት መቃወሚያው ተቀባይነት ሊኖረው ይገባል፡፡ ስለዚህ ከላይ በተጠቀሰው ጉዳይ ውስጥ በተከሳሽ በኩል በፍ/ስ/ስ/ህግ አንቀፅ 33(2) መሰረት ቀርቦ የነበረው መቃወሚያ ጉዳዩን በያዘው ፍ/ቤት ተቀባይነት አለማግኘቱ ስህተት ነበር፡፡[7] በእርግጥ በዚህ መቃወሚያ መሰረት ባይሆንም ጉዳዩ እስከ ፌደራል ጠቅላይ ፍ/ቤት ሰበር ሰሚ ችሎት ድረስ ደርሶ ተከሳሽ አሻናፊ ሊሆኑ ችሏል፡፡

[6] በፍ/ብሄር ህግ አንቀጽ 1731 መሰረት ውል በተዋዋይ ወገኖች መካከል ህግ ስለሆነ የጋብቻ ወል በተጋቢዎች መካከል ህግ ነው ማለት ይቻላል፡፡ የፍ/ብሄር ህግ አንቀጽ 1731(1) እና 1677(1) ይመልከቱ፡፡

[7]ከሳሽ በማንኛውም መንገድ ጉዳት ደረሰብኝ የሚል ከሆነ በሌላ መንገድ ካሳ መጠየቅ ይችል ይሆናል እንጂ የፈረሰን ውል እንዳልፈረሰ ቆጥሮ አዲስ የውል ይፍረስ ክስ ማቅረቡ ትክክል አይሆንም፤ አልነበረም፡፡

Printed By: ECSU Printing Press
+251 116 675505
ecsupress@gmail.com