THE LAW SOCIETY OF KENYA JOURNAL

LAW SOCIETY OF KENYA

VOLUME 21 2025

REPUBLIC OF KENYA

OFFICE OF THE CHIEF REGISTRAR
ADVOCATES SECTION

Notice to Advocates on
Notice of Intention to Apply for Practising Certificate in Special Cases under Section 25 of the Advocates Act

Advocates are hereby notified that **effective 1st November 2025**, all **Notices of Intention to Apply for Practising Certificate in Special Cases under Section 25 of the Advocates Act** shall be submitted and processed **exclusively** through the **Judiciary Advocates Management System (JAMS)**, accessible at ***https://jams.court.go.ke***.

Application Procedure:

1. Advocate to log in to his / her JAMS account.
2. Select '**Apply Notice of Intention**.'
3. Download the standard notice and statutory declaration provided.
4. Upload duly filled and commissioned statutory declaration with a signed notice.
5. Advocates Section will review and verify the application for compliance

    a. If the application is non-compliant, the same will be declined and the reason for decline indicated to enable the advocate submit a fresh application.
    b. If the application is compliant, the same will be approved by LSK and the advocate shall be notified accordingly via email and the JAMS portal.

Important Notice: As this is a newly introduced service, minor operational challenges may arise during the initial rollout. Constructive feedback is welcome and encouraged to help enhance system performance and user experience. Kindly direct all feedback to: ***advocatessection@court.go.ke***

The Law Society of Kenya Journal

Volume 21 2025

LAW SOCIETY OF KENYA

Notice- Call for Papers for the LSK Journal 2026

The Council of the Law Society of Kenya, through its Editorial Committee, invites members to submit articles for consideration in the **2026 Edition of the Law Society of Kenya Journal (LSKJ),** a peer-reviewed publication.

Submission Guidelines:

- Articles must comply with the LSKJ Instructions to Authors (accessible here, **LSKJ Instructions to Authors 2025.**
- Send submissions to **journal@lsk.or.ke** and include reliable telephone numbers and email addresses for communication.
- **Plagiarism is strictly prohibited** and will result in automatic rejection.
- We look forward to your contributions to this prestigious publication.

Printing and Layout by:

Magfre Enterprises Ltd.

P.O. Box 55944 - 00200

Email: info@magfre.co.ke

Table of Contents

DEFENDERS COALITION

SUPPORTING HUMAN RIGHTS DEFENDERS IN KENYA

WHO WE ARE

Defenders Coalition is the National Coalition of Human Rights Defenders in Kenya, established in 2007 to promote the safety, security, and well-being of Human Rights Defenders (HRDs). We are a trusted and professional organization dedicated solely to the protection of HRDs through capacity building, advocacy, and legal support. Our membership includes both organizations and individual defenders, and we are part of key regional and global human rights networks, including Defend Defenders and CIVICUS.

STRATEGIC PILLARS

- Enabling & safe civic space for HRDs
- Socio-economic Wellbeing of HRDs
- HRD Protection and Safety
- Instutitional Excellence

8000

Over 8,000 HRDs have benefited from our services on personal protection skills and rapid response.

WHO WE WORK WITH

Kenyan human rights organizations and Individual Human Rights Defenders
Defenders Coalition works with a diverse range of people and groups including:

- Indigenous people
- Women HRDs
- Journalists and bloggers
- PWDs
- Student Rights Defenders
- Social Justice Champions
- Environment and Land rights defenders
- Democracy and Good governance advocates
- LGBTQ+ rights defenders
- Veteran HRDs

Get in touch with us:

Emergency Toll Free Line: 0800 722292
Dial a Counsellor Toll free Line: 0800 724 280
Email: info@defenderscoalition.org

Engage with us Online

Facebook: Defenders Coalition
Tiktok: Defenders Coalition
Web: www.defenderscoalition.org
X (Twitter): @DefendersKE
Instagram: @defenderske

A Critical Analysis of Corporate Criminal Liability in Africa

Joseph Lutta*

Abstract

Broadly speaking, Africa is a haven of countless precious natural resources. This situation has attracted various corporate interests, which in turn were expected to spur political and socio-economic prosperity. However, this may not be the case as most countries are fraught with impunity and gross violations of human rights, which are mostly perpetuated by corporations. This dire situation is further exacerbated by the lack of credible institutions and political goodwill to prosecute corporations. However, the promulgation of the Protocol on Amendments to the Protocol on the Statute of the African Court of Justice and Human Rights opened an opportunity to redress this perennial state of impunity. In essence, it granted the proposed African Court on People and Human Rights the jurisdiction to prosecute corporations for international criminal offences. Therefore, it is incumbent upon all the material stakeholders to band together and support this strategy in restoring the rule of law and human dignity across the continent.

Keywords: *Corporations, Criminal Liability, Malabo Protocol, Business & Human Rights, Africa*

1.0 Introduction

Should corporations be prosecuted for committing transnational crimes in Africa?[1] However, this appears to be virtually implausible due to a myriad of challenges. According to Beth, African countries are either incapable or reluctant to prosecute multinational corporations within their jurisdiction.[2] If anything, these states attach a considerable premium to economic benefits rather than protecting human rights and dignity. This is because a vast majority of African states are economically impoverished, hence, they fear losing out on the economic windfall that comes with the operation of multinational

1 *Advocate of the High Court of Kenya LLB, Dip KSL. I am profoundly grateful for the preliminary remarks by the anonymous peer reviewers on the draft paper that was submitted for consideration by the Editorial Committee.

Diskant, Edward 'Comparative Corporate Criminal Liability: Exploring the Uniquely American Doctrine throughout Comparative Criminal Procedure' [2018] 118 Yale Law Journal 128.

2 Stephens, Beth 'The Amorality of Profits: Transnational Corporations and Human Rights' [2002] 20 (1) Berkeley Journal of International Law, 46.

corporations.[3]

Furthermore, corporations are considered too omnipotent to be controlled by most African governments due to a lack of the structures, institutions, and expertise to effectively prosecute corporate crimes. These myriads of legal *lacuna* have compelled some victims seeking redress in foreign jurisdictions with more sophisticated legal systems and well-developed jurisprudence on this subject matter.

For example, the family of late Nigerian activist Ken Saro Wiwa resorted to suing Shell Corporation in American courts after he was arbitrarily executed together with his eight compatriots known as the *Ogoni Nine* by the military Abacha regime in October 1995.[4] The crux of their case revolved around the fact that General Abacha's regime was supported by Shell, which enjoyed the exclusive rights to extract oil in the Niger Delta.[5]

This brief chronology forms the centerpiece of this paper. Firstly, it seeks to identify the legal position of corporate criminal liability in Africa with specific reference to Nigeria and Sierra Leone. More specifically, Nigeria offers a perfect example of how a weak legal system will compel victims to seek redress in a foreign jurisdiction, much like the victims from the Niger Delta who sue Royal Dutch Shell in the United States of America. On the other hand, Sierra Leone offers a two-prong legal issue to this subject matter. Firstly, it signifies the crime by omission if corporations like De Beers fail to screen out conflict diamonds from the market. In addition, it exposes the soft underbelly as how international criminal tribunals will overlook corporations when prosecuting perpetrators accused of gross human rights violation. Additionally, it analyses the proposed African Court of Justice, Human and People's Rights (hereinafter the African court) and its potential ability to prosecute corporate crimes in Africa. [6]

Structurally, this paper is divided into four portions. The first part gives a general overview of this paper. It underscores the position of corporate criminal

3 Duruigbo Emeka, 'The World Bank, Multinational Oil Corporations, and The Resource Curse in Africa' [2005] 26 (1) University of Pennsylvania Journal of international Economic Law, 46.

4 Smit Zyl Van Dirk, 'The Death Penalty in Africa'[2004] 4 African Human Rights Law Journal, 5.

5 Brown Cleverline, 'Environmental Crises in Nigeria and Extra Territorial Judicial Achievements: A Wake-Up Call for Nigerian Courts?' 11th June 2021, River State University.

6 African Union, 'Protocol on Amendments to the Protocol on the Statute of the African Court of Justice and Human Rights, Adopted on the 27 of June 2014 and Date of the last signature 3 July 2017 available at https://au.int/en/treaties/protocol-amendments-protocol-statute-african-court-justice-and-human-rights (last accessed on 15 December 2017).

liability in international criminal law. In the same vein, it encompasses a precise comparative study of the *Industrialist cases* at the

The Nuremberg Tribunal is the legal paragon of the criminal liability of corporations. The second portion encapsulates two case studies of Nigeria and Sierra Leone on the legal challenges besetting victims of corporate crimes in Africa.

The third part analyses the African court. This portion will argue that the establishment of this court is a progressive step towards the prosecution of corporations in Africa due to the accessibility of the judicial forum.[7] The fourth part shall outline the potential challenges and shortcomings that may impede the functionality of the court. It shall also encompass the concluding remarks from the author.

2.0 Corporate Criminal Liability and International Criminal Law

2.1 Can corporations be prosecuted under international criminal law?

By and large, corporations are not liable under international criminal law due to their idiosyncratic status as legal fiction and non-state actors.[8] However, the promoters and employees may be held responsible for committing offences on behalf of corporations.[9] This legal position was well captured in *US v Herman Goering,* where the Nuremberg tribunal stated:

> *"Hitler could not make aggressive war by himself. He had to have the co-operation of statesmen, military leaders, diplomats, and businessmen. When they with the knowledge of his aims, gave him their co-operation, they made themselves parties to the plan he had initiated. They are not to be deemed innocent because Hitler made use of them, if they knew what they were doing."*[10]

Secondly, the litmus test for any credible criminal justice system is its ability to uphold the rule of law irrespective of the stature of the offenders.[11] If political and military perpetrators are prosecuted for their actions what is

7 Adamski, (Maxi) Theresa 'The Alien Tort Claims Act and Corporate Liability: A Threat to the United States 'International Relations' 34 [2011] Fordham International Law Journal 1503.

8 Ronen, Yael 'Human Rights Obligation of Territorial Non-State Actors' (46) [2013] Cornel International Law Journal (46), 24.

9 Plomp, Caspar 'Aiding and Abetting: The Responsibility of Business Leaders under the Rome Statute of the International Criminal Court' 3 [2014] Utrecht Journal of International and European Law, 30 (79) 5.

10 Judgement of the Nuremberg International Military Tribunal 1946 (1947).

11 Kremnitzer, Mordechai 'A Possible Case for Imposing Criminal Liability on Corporations in International Criminal Law' [2010] Journal of International Criminal Justice, 8. 913.

so peculiar about corporations and their executives? Therefore, overlooking any form of human rights violation by corporations is tantamount to demeaning the international criminal justice system.[12]

Thirdly, corporations by virtue of their sheer magnitude and influence have the international obligation to protect human rights and dignity.[13] This inalienable obligation was amplified after the adoption of free trade agreements and globalisation expanded their geographical domain to the global south when socialism began to wither away.[14] For example in 2025, the annual turnover of top 8 Fortune 500 companies was surpassed $ 3 trillion which was equivalent to the entire GDP of Africa.[15]

On the opposite end of the spectrum, lies the countervailing argument that corporations unlike nation states are not parties to international law.[16] This legal quandary then begs the big question; 'if states ratify international legal documents why should corporations be indicted for actions that are well beyond their purview?'[17] If anything, punishing corporations is analogous to condemning innocent shareholders who are usually oblivious to the decision and resolutions of the management.[18]

Similarly, there is legitimate concern that using criminal sanctions is a counterproductive measure especially within the context of developing countries. Needless to say, a vast majority of people live way below the poverty line, hence they depend on employment opportunities

12 Engle, Karen 'Anti Impunity and the turn to criminal Law in Human Rights' [2015] Cornell Law Review, 100, 1070.

13 Weilert, Katarina 'Taming the Untamable? Transnational Corporations in United Nations Law and Practice' 14 [2010] Max Planck Yearbook of United Nations Law 445; Arato, Julian 'Corporations as Lawmakers' Summer [2015] Harvard International Law Journal 56 (2) 231.

14 Beck, Susan 'Meditating the Different Concepts of Corporate Criminal Liability in England and Germany' 11 (10) [2010] German Law Journal 11,10 1094; Golf, Le Pierrick 'Global Law: A Legal Phenomenon Emerging from the Process of Globalization' [2007] Indiana Journal of Global Studies 14 (1) 122.

15 https://eqvista.com/fortune-500-companies-in-the-us/ <last visited on 1st October 2025> These companies are Walmart, Amazon, United Health Group, Apple, CVS Health, Berkshire Herthaway, Alphabet and Exxon Mobil.

16 Alvarez, E. Jose 'Are Corporations "Subjects" of International Law?' [2011] Santa Clara Journal of International Law 9 (1), 20.

17 Slawotsky, Joel 'Corporate liability for violating international law under The Alien Tort Statute: The corporation through the lens of globalisation and privatisation' [2013] International Review of Law 6, 5.

18 Fisch, E. Jill 'Criminalisation of Corporate Law: The Impact on Shareholders and Other Constituents' [2007] Journal of Business and Technology Law 2 (1), 93.

offered by corporations.[19] Therefore, if corporations are beleaguered with swaths of indictments, regulations, and law suits there is likely to relocate thereby denying these people livelihood.[20]This line of argument is mostly propounded by the conservative and pro-business blocs who contend economic freedom is the precursor to political and social freedom. The most prominent proponent of this argument was the American economist and Nobel laureate Milton Friedman who argued the social responsibility of any business entity is to turn a profit.[21]

In summary, despite the glaring ideological differences it is fair to surmise there is an inextricable connection between corporate ventures and human rights.[22] Therefore, it is prudent to delineate the boundaries between these competing interests as a step towards protecting human rights.[23]

3.0 Schools of Thought on Corporate Criminal Liability in International Law

Wolfgang and Maas suggest two ways of holding corporations culpable under international criminal law.[24] Firstly, *'cooperation of businesses with military regimes and dictatorships'* occurs when corporations support military regimes in exchange for protection of their business interest.[25] This notion is further fragmented into three sub categories which are; 'profiting from state violence', 'facilitating international crimes of a regime by providing means of abuses' and 'direct support for repressions.'[26] The other category is known as *'corporations'*

19 Shleifer, Andrei 'The Age of Milton Friedman' [2009] Journal of Economic Literature 47 (1), 24.

20 Vazquez, Manuel Carlos 'Direct vs. Indirect Obligations of Corporations under International Law' [2003] Columbia Journal of Transnational Law 43, 929; Jennifer Westaway, Jennifer 'Globalisation, Transnational Corporations and Human Rights- A New Paradigm' [2012] International Law Research 1, (1) 63.

21 Friedman, Milton 'The Social Responsibility of Business is to Increase its Profits' New York Time Magazine, 13th September 1970 available at http://faculty.wwu.edu/dunnc3/rprnts.friedman.dunn.pdf (accessed on 23 December 2017).

22 Vest, Hans 'Business Leaders and the Modes of Individual Criminal Responsibility under International Law' [2010] Journal of International Criminal Justice 8, 852.

23 Mooney, Lelia 'Promoting the Rule of Law in the Intersection of Business, Human Rights and Sustainability' [2015] Georgetown Journal of International Law 46, 1136; Nolan, Justine 'Refining the rules of the Game: The Corporate Responsibility to Respect Human Rights' [2013] Utrecht Journal of International and European Law 30 (78),8.

24 Wolgang, Kaleck and Saage-Maap, Miriam 'Corporate Accountability for Human Rights Violations Amounting to International Crimes The Status Quo and Challenges' [2010] Journal of International Criminal Justice 8, 703

25 Ibid para 2.

26 Ibid pg. 705-707.

involvement in war zone and other conflict areas. [27]This situation transpires when businesses benefit by perpetuating internal conflicts in foreign jurisdictions. Specific examples include 'fuelling conflict through provision of goods and illicit funds,' providing military assistance' and 'intelligence services.[28]

Conversely, Ramasastry in her insightful paper *Corporate Complicity* offers a tripartite typology on this subject.[29]Firstly, *direct corporate complicity* occurs when corporations knowingly support states in violating customary international law.[30]This approach impugns corporations since they ought to preempt the 'likely consequences' of their actions. Under this banner she cites the example of the *Industrialist cases* where corporate executives were convicted for abetting the atrocities of the Nazi regime during the Second World War.

Secondly, *indirect corporate complicity* emanates when corporations benefit by investing in host countries guilty of gross violation of human rights.[31] She buttresses this notion with the landmark decision of *Doe v Unocal* where Burmese citizens sued Unocal an American energy conglomerate for gross violation of human rights by the Junta regime.[32]They averred the company knowingly entered into a joint oil and gas pipeline venture with the government of Myanmar despite being privy to its brutality.[33]In essence, this principle is dependent upon three major factors; a strong and symbiotic relationship between the corporation and the government, the corporation must be aware of the human rights violation and despite being aware of the atrocities it continues to honour the contract in furtherance of the regime.

Thirdly, *silence or inaction in the face of a host government's human rights violations* occurs when corporations knowingly invest in brutal regimes while overlooking their atrocities.[34] In essence, their sheer economic presence is construed to engender brutality since they generate revenue for the repressive government. A case in point is the massive economic investment by western corporations in apartheid South Africa and the fascistic reign of General Augusto Pinochet in

27 Ibid pg. 707 para 3.
28 Ibid 708.
29 Ramasastry, Anita 'Corporate Complicity; From Nuremberg to Rangoon – An Examination of Forced Labour Cases and Their Impact on the Liability of Multinational Corporation' [2002] Berkeley Journal of International Law 20 (1) 100.
30 Ibid pg. 102.
31 Ibid pg. 103.
32 963 F. Supp.880 (C.D. Cal 1997).
33 Becker, I. David 'A Call for the Codification of the Unocal Doctrine' [1999] Cornell Journal of Law Journal 32 (1) 184.
34 Ibid para. 6.

Chile.[35] In essence, corporations being genuine stakeholders in the economy can positively influence government policy to protect human rights. However, being a crime of omission makes it quite difficult to prove a guilty mind since framing public policies is beyond the province of corporations.

Another viewpoint argues corporations should be charged under principle of Joint Criminal Enterprise (JCE).[36] This legal standpoint argues voluntary participants belonging to a criminal syndicate possess common intention to commit an offence.[37] This doctrine was expounded upon by the International Criminal Tribunal for the Former Yugoslavia (ICTY) in *Prosecutor vs. Dusko Tadic*.[38] The tribunal affirmed its' unfettered discretion to convict people who may not have committed the offence but materially contributed to the commission of the offense as group with a common purpose.'[39]

This doctrine may be invoked if corporate officials jointly participate with host nations in repressing the citizens. Nonetheless, there are legitimate concerns its' applicability may be rendered nugatory considering the complexity of international criminal offences.[40] Despite this apprehension there is room for the prospective African court to elucidate this principle within the context of corporate criminal liability.[41]

The final legal dichotomy on this subject is the 'liberal versus romantics' school of thoughts. The liberal school of thought advocates accountability through broad definition of individual responsibility. In contradistinction, the romantics propound for institutional liability since corporations exercise unfettered control over their employees and actions. [42]

35 Cath, Colins 'Human Rights Trials in Chile During and After the 'Pinochet Years' [2009] International Journal of Transnational Justice 1; Bohler-Muller, Narnia 'Reparations for Apartheid-Era Human Rights Abuses: The Ongoing Struggle of Khulumani Support Group' [2013] Speculum Juris 1, 4.

36 Kyriakakis, Joanna 'Developments in international criminal law and case of business involvement in international crimes' Autumn [2012] International Review of the Red Cross 94 (887),991.

37 Bigi, Giulia 'Joint Criminal Enterprise in the Jurisprudence of the International Criminal Tribunal for the Former Yugoslavia and the Prosecution of Senior Political and Military Leaders: The Krajisnik case' [2010] Max Planck UNYB 14, 56.

38 IT -94-1-A 15th July 1999.

39 Ibid para. 172 of the judgement.

40 Catherine H. Gibson, H. Catherine 'Testing the Legitimacy of the Joint Criminal Enterprise in the ICTY: A Comparison of Individual Liability for Group Conduct in International and Domestic Law' [2008] Duke Journal of Comparative & International Law 18, 546.

41 Sliedregt, Van Elies 'Joint Criminal Enterprise as a Pathway to Convicting Individuals for Genocide' [2017] Journal of International Criminal Justice 5, 193.

42 Carsten, Stahn 'Liberals vs. Romantics: Challenges of an Emerging Corporate International Criminal Law' [2012] Case Western Reserve Journal of International Law, 50 (1) 100.

4.0 United Nations Norms of Responsibilities of Transnational Corporations and Other Business Enterprises with Regards to Human Rights

The norms were promulgated as a blueprint to incorporate the rule of law as part of the core values and practices for business organisations.[43] It contains five major principles;[44] *general obligations*, *right to equal opportunity and non-discriminatory treatment*, *right to security of person*, *right of workers, respect of national sovereignty and human rights,* and *obligations concerning consumer protection*.[45]

For brevity purposes, principles one, three, and five pertain to this paper because they triangulate among states, corporations, and international human rights law. Firstly, *general obligations* require transnational corporations operating within their territories to respect human rights.[46]

Conversely, the *right to personal security of a person* prohibits businesses from profiting from regimes that fail to safeguard human rights. Finally, *respect for national sovereignty and human rights* requires business entities to uphold the rules of law and public interest of the host countries.

However, this paper is hamstrung by its 'soft law' nature due to its persuasive undertones and the lack of any legal ramifications for the perpetrators.[47]

5.0 United Nations Guidelines on Business and Human Rights (UNGBHR)[48]

The UNGBHR was adopted by the United Nations Human Rights Council in 2011 in order to crystallise human rights within the realms of corporate responsibility.[49] As one of its brainchildren, John Ruggie stated that the

43 Weissbrodt, David and Kruger, Muria 'Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regards to Human Rights' [2003] American Journal of International Law 9, 902.

44 Surya Deva, 'UN's Human Rights Norms for Transnational Corporations and Other Business Enterprises: An Imperfect Step in the Right Direction?' [2004] ISLA Journal of International and Comparative Law 10, 503.

45 Ibid.

46 Pini Pavel Miretski, 'The UN's Human Rights Norms on the Responsibility of Transnational Corporations and Other Business Enterprises with Regards to Human Rights: A Requiem' [2012] Deakin Law Review 17 (1), 8.

47 Adeyeye, Adefolake 'Corporate Responsibility in International Law: Which Way to Go' [2007] Singapore Year Book of International Law and Contributors 11, 142

48 United Nations Human Rights Office of the High Commission, Guiding Principles on Business and Human Rights, New York and Geneva, 2011.

49 Nolan, Justine 'Refining the Rules of the Game: The Corporate Responsibility to Respect Human Rights' [2014] Utrecht Journal of International and European Law 30 (78), 8.

guidelines are a means to an end by defining the legal parameters intersecting between business and human rights.[50] The UNGBHR consists of thirty-one principles, which stand on three major pillars: *the duty of the state to protect human rights*, *corporate responsibility to respect human rights,* and *access to remedy*. [51]

The first pillar requires the states to implement strong regulatory measures and policies that ensure businesses respect and uphold human rights.[52]More specifically, foundational principles 1 and 2 echo the duty of states to avert abuse of human rights within their jurisdiction.[53] Similarly, principle 3(a) requires states to realign their general regulatory policies to ensure business entities observe fundamental rights and freedoms.[54]

Inversely, the *principle of corporate responsibility to respect human rights* obliges businesses to 'know and show' respect for human rights.[55] More succinctly, this duty is enshrined in guiding principle 11, which states:

> *"Business enterprises should respect human rights. This means they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."*[56]

Thereafter, guideline 12 compels businesses to respect the minimum standards of human rights as prescribed by the various international instruments, most salient being the International Covenant on Civil and Political Rights (ICCPR) and International Covenant on Economic, Social and Cultural Rights (ICESCR).[57]

Guideline principle 13 is equally significant for outlining the dual obligation for businesses to address human rights concerns and avoid engaging in ventures

50 John Ruggie, 'The Social Contract of the UN Guiding Principles on Business and Human Rights' Corporate Responsibility Initiative Working Paper Number 67 Cambridge, Ma: John F. Kennedy School of Government, Harvard University.

51 Ibid at 3.

52 Backer, Cata Larry [2015] 'Moving Forward the UN Guiding Principles for Business and Human Rights: Between Enterprise, Social Norm, State Domestic Legal Orders and the Treaty Law That Might Bind Them All' [2015] Fordham Journal of International Law 38 (2), 469.

53 Ibid pg 3.

54 Ibid pg 4

55 Rachel, Davis 'The UN Guiding Principles on Business and Human Rights and Conflict-affected area: state obligations and business responsibilities' Autumn [2012] International Review of the Red Cross, 94 (887), 970.

56 Ibid. at 13

57 Ibid at 13.

that may result in the violation of these rights.[58] Closely related is guideline principle 15, which requires business enterprises to formulate and implement policies to safeguard human rights.[59]

The principal objective of the third pillar empower victims to secure remedies through judicial and non-judicial means.[60] These remedies, which are scattered across principles 25-31, revolve around the primary obligation of states to offer the judicial, legislative, administrative, and any other appropriate recourse.[61] This legal obligation is intertwined with principle 26, which outlines the responsibility of states to eliminate barriers that could deny victims' access to justice.[62]

Similar to the UN Norms of 2001, these guidelines are soft laws in nature because they do not constitute legally binding obligations. Consequently, there is reasonable skepticism about its viability considering the absence of an implementation mechanism among the member states.[63] Despite this, some member states have begun adopting these guidelines towards the progressive realisation of the overall objectives.[64]

6.0 The Nuremberg Tribunal Cases

6.01 Brief Background

The Nuremberg tribunal was empaneled in 1945 to prosecute the members of the Nazi regime for the gruesome atrocities committed during the Second World War.[65] The statute outlined the major crimes as: crimes against peace, war crimes, and crimes against humanity.[66] Furthermore, it defined offenders to encompass 'leaders, organisers, instigators and accomplices' with common conspiracy to commit the offences.[67]This

58 Ibid at 14.

59 Ibid at 15.

60 John, Gerard Ruggie and John, F. Shearman III 'The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights: A Reply to Jonathan Bonnitcha and Robert McCorquadale' [2017] European Journal of International Law 28 (3), 923.

61 Ibid pages 27-29.

62 Ibid pg. 31.

63 Noura, Barakat 'The U.N. Guiding Principles: Beyond Soft Law' Spring [2016] Hastings Business Law Journal 12 (3) 597.

64 Douglas, Cassell and Anita, Ramastsry 'White Paper: Options for a Treaty on Business and Human Rights' September [2016] Notre Dame Journal of International and Comparative 6 (1) 9.

65 Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis. Signed at London on the 8th of August 1945 (Nuremberg Charter); Levy, Daniel and Sznaider, Natan 'The Institutionalising of Cosmopolitan Morality: The Holocaust and Human Rights' June [2004] Journal of Human Rights 3 (2), 147.

66 Ibid. clause 6.

67 King, T Henry Jr. 'Nuremberg and Crimes against Peace' 41 (2) [2009] Case Western Reserve Journal

broad definition expanded the scope of perpetrators to include a cartel of tycoons who supported the regime in exchange for commercial and political gains.[68]

6.02 Flick Case [69]

The defendants were a clique of wealthy businessmen known as 'Circles of friends of Himmler.'[70]They were accused of making generous contributions to Heinreicht Himmler and his *Schutzstaffel* (SS) organisation. This sinister but grotesque paramilitary unit was accused of being instrumental in the 'extermination of Jews.' In exchange for the contributions, these businessmen benefited by forcefully acquiring Jewish-owned businesses and free labour supplied from inmates interned in concentration camps. Consequently, three of them were found guilty of aiding and abetting the criminal activities of the *SS*.[71] The tribunal stated, *'One who knowingly contributes to the support of a criminal organisation must be deemed to be if not a principal, certainly an accessory to such crimes.*'[72]

6.03 Ministries Case[73]

One of the offenders was Karl Rasche a successful banker and board member of the Dresdner Bank. He was accused of actively financing the 'Circle of friends of Himmler friends' and several corporations that profited from slave labour supplied from inmates detained in concentration camps scattered across Eastern Germany and Poland.[74]

The tribunal pondered whether loaning money to a business entity that violates international law is a crime. The tribunal observed despite the reprehensible nature of the transaction, the accused could only be condemned from a 'moral standpoint'. Nonetheless, he was convicted of plundering public and private property after forcefully acquiring

of International Law41 (2), 273.

68 Lustig, Doreen 'The Nature of the Nazi State and The Question of International Criminal Responsibility of Corporate Officials at Nuremberg: Revisiting the Franz Neumann's Concept of Behemoth at the Industrialist Trials' Summer (2011) New York University Journal of International Law & Politics 43, 965.

69 Flick Trial United States Military Tribunal, Nuremberg 20th-22nd December 1947.

70 The accused persons were Friedrich Flick, Otto Steinbrink, Bernhard Weiss, Odillo Burkhat, Konrad Kaletsch and Herman Terberger.

71 Those convicted were Friedrich Flick, Otto Steinbrink and Bernhard Weiss.

72 Vest, Hans 'Business Leaders and the Modes of Individual Criminal Responsibility under International Law' 8 (2010) Journal of International Criminal Justice 854.

73 *United States of America v Ernst von Weizsacker et al.* US Military Tribunal Nuremberg, Judgement delivered on the 11th of April 1949.

74 Pg 226 of the judgement.

Jewish-owned businesses in Czechoslovakia.[75] In light of the gravity of his offences, he was subsequently sentenced to seven years' imprisonment on both counts.[76]

This landmark decision expounds on the legal intricacies surrounding offenders accused of financing gross violations of human rights. Although it was tremendously difficult to impart a guilty mind upon the accused, the tribunal should have gone a step further and interrogated the principle objective behind the transaction. Considering the autocracy of the Nazi regime, the only permissible line of defence would have been coercion. However, this excuse could not suffice since the accused, being a professional, failed to undertake meticulous due diligence before approving the credit. Consequently, failure to discharge this onerous duty was sufficient to establish his intention to commit the offences.

6.04 The Zyklon B case[77]

The offenders were Bruno Tesch, Karl Weinbacher, and Joachim Drosihn, the Chief gas technician. They were jointly charged with supplying the *SS* with a poisonous chemical substance called *Zyklon B* that was used to exterminate Jews detained at the death camps in Auschwitz and Birkenau. They nonetheless pleaded not guilty since they presumed the buyers were going to use the chemical to fumigate the camps. Nonetheless, the first two defendants were convicted and sentenced to death by hanging since they were well aware the substance was being used on humans.[78] As for Drosihn, he was acquitted since he was at the very tail end of the chain of transaction, hence, he could not comprehend the intention of his superiors and their accomplices.

6.05 Krupp case[79]

The main accused was Alfried Krupp, a prominent steel magnate, close confidante, and financier to Hitler. Upon ascending to power, Hitler had passed a special executive order known as *Lex Krupp,* which granted him absolute ownership of the steel conglomerate Krupp A.G.[80] During the occupation of foreign territories, he forcefully acquired Jewish-owned steel companies and benefited from free labour supplied by detainees in the

75 Pg 332 of the judgement.
76 Pg 399 of the judgement.
77 Case Number 9 the trial of Bruno Tesch & others British Military Court, Hamburg, 1-8 March 1946.
78 Pg. 96-102 of the judgement.
79 Case Number 57 United States Military Tribunal 14th August 1947- 29th July 1949.
80 Reichsgesetzblatt 1943 I, 655f.

concentration camps. Upon trial, he was ultimately convicted of all counts and sentenced to 12 years' imprisonment.

Cumulatively, these decisions dispel the myth that corporations and their employees cannot be held culpable under international criminal law.[81]

7.0 The African Context

7.1 Are natural resources a curse or blessing?

On a more abstract level, natural resources are the boon and bane of the African continent.[82] On the one hand, they signify the socio-economic potential of the continent. According to a 2015 economic report authored by the African Development Bank (ADB), the continent is likely to generate approximately $ 30 billion in annual revenue within the next 5 years.[83] This colossal sum is emblematic of the continent's prospects as an undisputed economic powerhouse.

Conversely, these resources are stereotyped as 'bad omen' for plaguing the continent with political volatility, carnage, and soaring poverty levels.[84] Since time immemorial, Africa has been a haven of plunder and repression by both foreign countries and corporations.[85] This impunity hit a peak after the Berlin Conference of 1885, which paved the way for the colonisation of Africa by European powers. Nonetheless, after decolonisation, there was profound optimism that the populace would finally enjoy the benefits of their resources.[86] However, this utopian dream turned ominous after most countries were embroiled in civil wars, grotesque carnage, and abject poverty.[87] This political disintegration transpired despite the continent being signatory to a spectrum of international human rights instruments.[88]

81 Kolieb, Jonathan 'Through the Looking-In-Glass: Nuremberg's Confusing Legacy on Corporate Accountability under International Law' [2017] American University Law Review 32 (2), 571.

82 African Development Bank, *Africa's Natural Resources: The Paradox of Plenty* (2007) 97.

83 African Development Bank Group, African Natural Resources Center (ANRC) Strategy 2015-2020, June 2015 1.

84 Shaxson, Nicholas 'Oil, Corruption and the resource curse' (2007] International Affairs 83 (6), 1124.

85 Mbote, Kameri Patricia and Cullet, Philippe 'Law, Colonialism and Environment Management in Africa' [1997] Review of European Community and International Environmental Law, 6 (1), 23.

86 Okon, Etim 'Kwame Nkrumah: The Fallen and Forgotten Hero of African Nationalism' [2014] European Scientific Journal, 10 (17), 56.

87 El-Obaid, Ahmed El-Obaid and Appiagyei-Atua, Kwadwo 'Human Rights in Africa- A New Perspective on Linking the Past to Present' [1996] McGill Law Journal, 41, 827.

88 Universal Declaration on Human Rights Adopted by the United Nations General Assembly resolution 217 A (III) of 10 December 1948; International Covenant on Civil and Political Rights Adopted by the General Assembly of the United Nations on 19 December 1966 Optional Protocol Adopted by the General Assembly of the United Nations on 19 December 1966; International Covenant on Economic Social and Cultural Rights Adopted and Opened for Signature, ratification and accession by

This lamentable scenario, informally described by economists as the 'paradox of plenty', is the common denominator among most mineral-dependent countries in Africa.[89]

Despite this dystopian outlook, corporations continue to court these tyrannical regimes in exchange for access to resources. For instance, from 2008 to 2010, the continent lost close to $ 63.4 billion in illicit profits generated by corporations from armed conflicts.[90] This worrisome situation exemplifies how corporations compound the culture of impunity and the need for credible structures and policies to combat this situation.[91]

8.0 Legal Challenges to the Prosecution of Corporate Criminal Liability in Africa

8.01 Prosecution of Corporations in Foreign Jurisdiction

In Africa, victims of human rights violations are usually unable to secure legal remedies against corporate perpetrators. This legal conundrum is best portrayed by the cases filed by the Ogoni people in Niger Delta against Shell.[92] Despite their proximity to vast oil reserves, this region was entangled in a vicious cycle of poverty and impunity.[93] Furthermore, Shell had 'overexploited' the commodity in disregard of environmental concerns, leading to widespread oil spills and gas flares.[94] This, in turn, led to the contamination of fishing grounds and arable land, which had adverse effects on the health and livelihood of the native population.[95]

---

the General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 3 January 1976, in accordance to article 27.

89 Ibid.

90 Tsabora, James (2014) 'Illicit Natural Resource Exploitation by Private Corporate Interests in Africa Maritime Zone during Armed Conflict' Spring [2014] Natural Resources Journal 54 (1), 183.

91 Udombana, J. Nsongurua 'Toward the African Court on Human and People's Rights: Better late than Never' [2000] Yale Human Rights and Development Law Journal 3 (45), 54.

92 Yusuf, O. Hakeem 'Oil on trouble waters: multi-national corporations and realising human rights in the developing world, with specific reference to Nigeria' [2008] African Human Rights Law Journal 8, 86.

93 Boele, Richard, Fabig, Heike and Wheeler, David 'Shell, Nigeria and the Ogoni, A Study in Unsustainable Development: The Story of Shell Nigeria and the Ogoni People- Environment, Economy Relationships: Conflict and Prospects for Resolution' [2001] Sustainable Development 9, 77.

94 Konne, Rachel Barisere 'Inadequate Monitoring and Enforcement in the Nigerian Oil Industry: The Case of Shell and Ogoniland' [2014] Cornell International Law Journal 47, 184.

95 Ebeku, S.A. Kaniye 'The Right to a satisfactory environment and the African Commission' [2003] Africa Human Rights Law Journal 3, 157; Ukala, Eferiekose 'Gas flaring in Nigeria's Niger Delta: Failed Promises and Reviving Community Voices [2011] Washington Lee Journal of Energy, Climate and Environment 97 (2), 97.

Nonetheless, the gravamen of this dispute revolved around the summary execution of the leaders of the Movement for the Survival of the Ogoni People (MOSOP) by the regime of General Sani Abacha.[96] In 2006, the families of two of the leaders, Ken Saro Wiwa and Ben Kiobel, sued Royal Dutch Shell in the United States under the Alien Tort Claims Act.[97] This federal statute permits foreign litigants to sue American citizens for gross violation of the 'laws of nations' or treaty.[98]

These victims argued Shell was complicit in the atrocities of the Abacha regime by offering financial support, military intelligence, and bribing the witnesses who testified against the Ogoni six. The offences committed included extrajudicial killing, crimes against humanity, torture and cruel treatment, arbitrary arrest and detention, forced exile, and plunder.[99]

As anticipated, the cases underwent their fair share of twists and turns after Shell raised a series of preliminary objections to dismiss the suit for want of jurisdiction. In the *Wiwa* case, the district court dismissed the case under the principle of *forum non convenience*.[100] The judge reasoned the case should have been filed either in Britain or the Netherlands, where the defendant was domiciled, a decision which prompted the plaintiffs to appeal.[101] In allowing the appeal, the judges concurred that the statute granted the plaintiffs a wide latitude to file their claim in America. Nonetheless, Shell agreed to settle the matter for $ 15.5 million and establish trust on behalf of the Ogoni people.[102]

Similarly, one of the Ogoni nine activists who was executed together with Wiwa was Dr. Barinem Kiobel. His widow, Esther Kiobel, filed a similar suit against Royal Dutch Shell in the Southern District of New York.[103] Just like the Wiwa family, she argued that by virtue of the Alien Tort Act (ATS)

96 Umezurike, Augustine Samuel and Lucky, E. Asuelime 'Exploring Diplomatic Crisis of Nigeria and South Africa between 1994-2013' March [2015] Academic Journal of Inter Disciplinary Studies 4 (1), 67.

97 28 USC 1350 ATS.

98 Shapiro, Dorothy 'Kiobel and Corporate Immunity under the Alien Tort Statute: The Struggle for Clarity Post Sosa' March [2011] Harvard International Law Journal 52, 210.

99 Smith, Amy and Lowery, Carrie 'Kiobel v Royal Dutch Shell Petroleum Co: Radical Revision or Original Intent of the Alien Tort Statute' Fall [2014] Southern Law Journal, XXIV 292.

100 Barrett, L. Edward, 'The Doctrine of Forum Non-Convenience' [1947] California Law Review 35 (3), 380.

101 Wiwa v Royal Dutch Petroleum Co. 226 F. 3d.

102 Fellmeth, Xavier Aaron 'Wiwa v Royal Dutch Shell Co: A New Standard for the Enforcement of International Law in U.S. Courts?' [2002] Yale Human Rights and Development Journal 5 (1), 249.

103 458 F. Supp 2d SDNY (2006).

granted the *locus standi* to sue Shell for aiding and abetting the atrocities of the Abacha regime. Conversely, Shell raised a preliminary objection on the grounds that non-state actors like Shell could be held culpable under customary international law.[104] In upholding the objection, the trial court concurred with the defence counsel that the norms of customary international law never envisaged non-state actors like Shell.

When the plaintiffs appealed to the Second Circuit Appeals Court, the Judges upheld the decision of the trial court holding that 'corporate liability' is neither discernible nor recognised under customary international law.[105]

Relentless, the widow appealed the decision to the Supreme Court reiterating the merits of her case just like the family of Ken Wiwa.[106] However, in a 5-4 majority decision the matter reached the Supreme Court, it was held that the framers of the ATS never envisaged it as a tool for enforcing international legal norms in America. In addition, the majority judges relied on the presumption of extra territorial application to dismiss the suit. This doctrine states that if a statute does not provide for direct extra territorial application then none exists.[107] Furthermore, if American courts exerted their jurisdiction over the matter then it would violate the doctrine of separation of powers since congress had enacted the Torture Victim Protection Act which offered the appropriate avenue and forum to deal with similar claims.[108] In their view, this statute and not the ATS was the panacea to the nature of grievances lodged by the plaintiffs.[109] This decision defeated the letter and spirit of the statute, which intended to eliminate the legal challenges encountered by foreign victims of American corporations.[110]

Despite the outcome, in 2022, the Kiobel and 3 other widows filed another claim in the District Court at Amsterdam, Netherlands, where Shell NV, which is part of Royal Dutch Shell, is domiciled.[111] They held a

104 Ibid.

105 *Kiobel et al vs Royal Dutch Shell* 621 F. 3d 111 (2D. Cir. 2010).

106 565 US 961 (2010).

107 Green, M. Jennifer 'The Rule of Law at a Crossroad: Enforcing Corporate Responsibility in International Investment through the Alien Tort Statute' [2014] University of Pennsylvania Journal of International Law 34,1099.

108 28 US 1350.

109 Ku, G. Julian 'Kiobel and the Surprising Death of Universal Jurisdiction under the Alien Tort Statute' [2013] American Journal of International Law 107, 837.

110 Simmons, Marco 'Kiobel v Royal Dutch Petroleum: A Practitioner's Viewpoint' [2013] Maryland Journal of International Law 28 (1), 30.

111 *Kiobel vs Royal Dutch Shell & others* C-09-540872-HA ZA-17-1048.

similar argument that Shell had bribed the witnesses who had testified in the military tribunal against their husbands in 1995. However, the court held that the claimants had failed to prove their case because there was no evidence that witnesses were either coerced or bribed by the defendants.

These cases epitomised how corporations can flex their financial muscle and manipulate the legal system to their advantage.[112] Often, corporations are endowed with the financial resources to secure the best legal representation to neuter any allegations of human rights violations. Nevertheless, should these perpetrators exhaust all possible obstacles, then they resort to compromise the matter without admission of liability. In the *Wiwa case*, the $15 million settlement was seemingly modest compared to then Shell's quarterly gross profit of $ 3.9 billion.[113]

9.0 The Viability of the African Commission on Human and Peoples Rights in Enforcing Remedies for Gross Violation of Human Rights

The African Commission on Human and Peoples Rights was established on 2nd November 1987 in Banjul, Gambia. [114] By and large, it was bestowed with three major obligations: to protect human and peoples' rights, promote human and peoples' rights, and interpret the African Charter on Human and Peoples' Rights. Indeed, this body has been instrumental in examining whether states have discharged their obligations in terms of the protection and promotion of human rights. [115]

For instance, a human rights organisation called Socio-Economic Rights Action Center (SERAC) lodged a formal communication against Nigeria with the commission.[116] They argued the Nigerian government had failed to protect the rights of the Ogoni people from the atrocities committed by Shell. In its ruling, the commission agreed that the actions violated the charter and appealed to the Nigerian government to improve the welfare of the Ogoni people.

112 Newman, Dave 'Litigation Update Wiwa v Royal Dutch Shell' Summer [2002] Sustainable Development Law & Policy 2 (2) 3; Alford, P. Roger 'Human Rights after Kiobel; Choice of Law and Rise of Transnational Tort Litigation' [2014] Emory Law Journal 63, 1112.

113 Ed Crooks 'Shell profits rise to 60% to 4.8 billion' *Financial Times* 28 April 2010 *Financial Times* available at https://www.ft.com/content/111326d0-5298-11df-a192-00144feab49a (accessed on 21 of December 2017).

114 See https://achpr.au.int/en last visited on 1st October 2025.

115 Sabelo Gumedze, 'Bringing communications before the African Commission on Human and Peoples' Rights' [2003] African Human Rights Law Journal 3, 121.

116 *SERAC & Another v Nigeria* (2001) AHRLR 60.

This case exposed the glaring shortcomings of the commission in punishing African states for failing to uphold the rule of law. Its only recourse was appealing to the government to improve the living conditions and compensate the victims. Consequently, the government took close to 15 years to comply with the order, an act which demonstrated the bureaucratic challenges that bedevil the implementation of these orders.[117]

10.0 Inadequacy of Special Criminal Courts to Offer Reparations for Victims of Human Rights Abuses Perpetuated by Corporations in Africa

This lacuna is illustrated by the interface between De Beers Group and conflict diamonds ('blood diamonds') that fuelled the bloody civil war in Sierra Leone. [118] This conflict pitted the government forces of Sierra Leone against a rebel movement known as the Revolutionary United Front (RUF), led by Fodhay Sanko. Sanko was supported by then-Liberian President Charles Taylor, who was interested in the lucrative diamond mines in the South West region of Kono. [119]

What began as a minor insurgency snowballed into a gruesome and protracted civil conflict that left close to 75,000 civilians dead while displacing almost 2.4 million people.[120] The RUF resorted to barbaric war tactics, including mass amputations, sexual violence, kidnapping, and forceful conscription of child soldiers.[121] In 1999, the United Nations (UN) brokered a temporary cease-fire after parties agreed to form a coalition government, which granted the RUF the mandate to control the diamond mines.[122]

However, the RUF breached the peace treaty, which prompted the UN to empanel a special court that indicted Taylor, Sanko, and other RUF leaders

117 Ezeudu, Martin Joe 'Revisiting Corporate violations of Human Rights in Nigeria's Niger Delta region: Canvassing the potential role of the International Criminal Court' [2011] Africa Human Rights Law Journal 11, 42.

118 Akinranade, Babafemi 'International Humanitarian Law and the Conflict in Sierra Leone' [2001] Notre Dame Journal of Law, Ethics and Public Policy 15 (2), 396.

119 Howard, Audrie 'Blood Diamonds: The Success and Failure of the Kimberley Process Certification Scheme in Angola, Sierra Leone and Zimbabwe' [2015] Washington University Global Studies Law Review 15 (1), 142.

120 Forest, Laura 'Sierra Leone and Conflict Diamonds: Establishing a Legal Diamond Trade and Ending Rebel Control over the Country's Diamond Resources' [2011] Indiana International & Comparative International Law Review 11 (3), 637.

121 Manchuk, Iryna 'Confronting Blood Diamonds in Sierra Leone: The trial of Charles Taylor' Spring/ Summer [2009] Yale Journal of International Affairs 88.

122 Peace Agreement between the Government of Sierra Leone and The Revolution United Front of Sierra Leone 12 July 1999 available at https://peacemaker.un.org/sites/peacemaker.un.org/files/SL_990707_LomePeaceAgreement.pdf (accessed on 28 December 2017).

for war crimes and crimes against humanity.[123] Although Sanko died while in detention, Taylor was ultimately convicted of war crimes and crimes against humanity and sentenced to 50 years' imprisonment.[124]

However, the missing link to this chain of transactions was the instrumental role played by De Beers Group in perpetuating the conflict. This South African Company controls close to 60% of the global diamond industry, thereby determining the market price for diamonds by regulating the supply.[125] As Lucina Saunders notes, corporate actors facilitate diamond trade in illicit diamonds either directly or indirectly from insurgent groups.[126]

During the conflict, the RUF used uncut diamonds as a commodity of trade in exchange for arms, foodstuffs, and narcotics.[127] De Beers had the principal obligation to block the trading of conflict diamonds in the global market. This obligation stems from the fact that, by virtue of being the biggest player in an exclusive and well-regulated industry, it could proscribe the sale of these diamonds. However, by failing to screen out the trade of illicit diamonds in such a specific and controlled industry then it perpetuated the conflict by offering the rebels a black market.

In hindsight, the criminal tribunal succeeded in convicting individuals like President Charles Taylor, who bore the greatest political responsibility for the conflict. However, it appears the farmers might have overlooked the critical role that was played by the diamond dealers in perpetuating the conflict. Ultimately, this loophole signifies the importance of reparation clauses as a mechanism for dealing with corporate criminal responsibility in armed conflicts.

11.0 The Case for a Continental Criminal Court

The International Criminal Court (ICC) adjudicates international criminal law matters globally . However, this framework has been assailed for being biased and political because most of the accused persons are Africans.[128]

123 Statute of the Special Court for Sierra Leone establishment by an agreement between the United Nations and the Government of Sierra Leone pursuant to Security Council resolution 1315 (2000) of 14 August 2000 available at http://www.rscsl.org/Documents/scsl-statute.pdf (accessed on 28 December 2017).

124 *Prosecutor v Charles Ghankay* Taylor SCSL-03-01-A. 23 September 2013.

125 Chang, So Young et al. 'The Global Diamond Industry' Fall [2002] Chazen Web Journal of International Business 8-7.

126 Saunders, Lucinda 'Rich and Rare are the Gems they war: Holding De Beers Accountable for Trading Conflict Diamonds' [2004] Fordham International Law Journal 24 (4), 1428.

127 Feldman, L. Daniel 'Conflict Diamonds, International Trade Regulation, and the Nature of Law' [2003] University of Pennsylvania Journal of International Economic Law 24 (4) 835.

128 Murungu, Bhoke Chacha 'Towards a Criminal Chamber in the African Court of Justice and Human

Furthermore, the court is considered 'imperialistic' for being controlled by the veto powers of the Security Council, which are considered the greatest violators of human rights.[129] Consequently, the African Union (AU) mooted the idea of establishing a continental court to circumvent these challenges.[130]

11.01 Brief Chronology of the Court

The court established by the African Charter on Human and Peoples' Rights that crystallised international human rights at the continental level.[131] The charter also provides for the quasi-judicial African Commission on Human Rights as the adjudicator of human rights issues.[132] However, in 1998, the Organisation of African Unity (OAU) set up the African Court on Human and Rights as the continental judicial organ.[133] When the OAU evolved into the AU, the African Court of Justice was established as the principal judicial organ.[134]

In 2004, the AU proposed to integrate the African Court of Justice and the African Court of People and Human Rights into a single institution called the African Court of Justice, People and Human Rights.[135] This proposal was subsequently approved in 2008 during the AU Heads of State summit in Sharm El-Sheikh, Egypt.[136] In 2014, the Malabo summit promulgated the annexed statute amendments, which were opened for ratification by the member states. Pursuant to Article 8, the protocol shall come into effect 30 days after ratification by at least 15 member states.

Rights' November [2011] Journal of International Criminal Justice 9 (5), 1081.

129 Art 13-15 of the Rome Statute; Margret M. de Guzman 'Choosing to Prosecute: Expressive Selection at the International Criminal Court' [2012] Michigan Journal of International Law 33 (2), 274.

130 12th Ordinary Session of the African Union February 2009, Addis Ababa, Ethiopia.

131 African Charter on Human and People's Rights, adopted on the 27th of June 1981, OAU Doc. CAB/LEG/67/3 Rev. 5,21 I.L.M. 58 (1982), entered into force on the 21st of October 1986.

132 Article 62 of the ACPHR.

133 Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, June 10, 1998, OAU Doc. OAU/LEG/EXP/AFCHPR/PROT (III) (entered into force Jan. 25 2004) [ACHPR].

134 Protocol of the Court of the Justice of the African Union; Konstaninos D. Magliveras and Gino L. Nadi 'The African Court of Justice' 2006 Max Planck 189.

135 Report on the Decision of the Assembly of the Union to merge the African Court on Human and Peoples' Rights and the Court of Justice of the African Union, Executive Council, Sixth Ordinary Session, 24th-28th January 2005, Abuja , Nigeria EX.CL/162, pg 1-2.

136 Protocol on the Statute of the African Court of Justice and Human and People's Rights, adopted by the 11th Ordinary Session of the Assembly of the African Union, Sham Al Sheikh Egypt. 1st July 2008.

11.02 Structure of the Court

Generally, the court will comprise separate chambers dealing with general affairs, human and people's rights, and international criminal law (ICL).[137] The general affairs division shall determine all matters referred under Article 28 of the statute except those allocated to the other divisions.[138] Conversely, the Human and People's Rights division shall determine all issues with regard to human rights.[139] Finally, the ICL section shall adjudicate the criminal offences as specified in the statute.[140]The court shall comprise 15 judges who shall be reputable, experienced, and revered scholars in international law who shall serve for a non-renewable term of nine years.[141]

11.021 Chambers

The ICL is stratified into three chambers: pre-trial, trial, and appellate chambers. The appellate chamber shall determine matters on grounds of errors of procedure, law, and facts.[142] Furthermore, there shall be the office of the general prosecutor supported by two deputies and an office for the defence counsels.[143] In terms of sentencing, the court shall have the mandate to order both custodial sentences and payment of fines.[144] Furthermore, the judges shall have the supplementary authority to order perpetrators to pay compensation and reparations to their victims.[145]

11.022 Referral of Cases and Rights of the Accused

The cases may be referred to the court by the prosecutor, member states, Assembly of Heads of State and governments, the Peace and Security Council of the AU, private citizens from member countries who have ratified the Protocol, and NGO's with observer status by the AU.[146]Akin to any other criminal tribunals, the accused shall be accorded the relevant legal rights.[147] Article 48 B provides for the principle of individual criminal responsibility, which is pivotal in

137 Ibid article 16.
138 Ibid. article 17 (1).
139 Ibid Article 17 (2).
140 Ibid Article 17 (3).
141 Ibid Article 8.
142 Ibid Art 18 (2).
143 Ibid Article 22C.
144 Ibid Article 43A.
145 Ibid Article 45.
146 Ibid Article 29 and 30.
147 Ibid Article 46A of the Statute.

prosecuting offences committed by group offenders.[148] The Protocol also affirms that no person shall be exonerated from subsequent criminal proceedings by virtue of their position.[149] The Statute also recognises the principle of command responsibility, which holds superiors accountable for the actions of their subordinates.[150]

11.023 Offences

The court has an 'expanded jurisdiction' that entails a continuum of fourteen offences, including genocide, crimes against humanity, war crimes, crimes of aggression, human trafficking, drugs and hazardous wastes, piracy, corruption, money laundering, mercenaries, unconstitutional change of government, and terrorism.[151] This jurisdiction may be expanded by the Assembly upon consensus among member states.[152] This broad mandate is a wide deviation from other international criminal tribunals whose parameters are restricted to genocide, crimes of aggression, war crimes, and crimes against humanity.[153]

11.024 Corporate Criminal Liability under the Malabo Protocol

This legal concept is one of the features of the court that can exercise jurisdiction over both natural and legal persons.[154] Furthermore, paragraphs 3 and 4, which stipulate criminal intent may be imparted upon a corporation through 'actual or constructive knowledge' if the relevant information was well within its knowledge.[155] Aggregate knowledge means that an organisation might know a fact or situation even if the same was scattered across various officials. Conversely, constructive knowledge avers the organisation not only possessed the information but the culture 'positively promoted' the commission of

148 Stephenson, J. Pamela (2014) 'Collective Criminality and Individual Responsibility: The Constraints of Interpretation' [2014] Fordham Journal of International Law 37 (2) 513.

149 Ibid Article 46 B (2) of the Statute.

150 Ibid Article 46 B (3) of the Statute.

151 Ibid Article 28A (1) of the Statute.

152 Ibid Article 28 B of the Statute.

153 Sirleaf, Matiangai 'The African Justice Cascade and the Malabo Protocol' March [2017] International Journal of Transitional Justice 11,9; Gwam, Uchenna Cyril 'Human Rights Implications of Illicit Toxic Waste Dumping from Developing Countries Including The USA, Especially Texas to Africa, In Particular Nigeria' [2013] Thurgood Marshall Law Review 38, 247.

154 Joanna Kyriakis, 'Article 46 C: Corporate Criminal Liability at the African Criminal Court' in Charles C. Jalloh, Kamari M. Clarke and Vincent O. Nmehielle, *The African Court of Justice and Human and People's Rights in Context: Development and Challenges* Cambridge [2019], 797.

155 Ibid. Article 46 C (3) and (4) of the Statute.

the offence. [156]

This legal position reverberates with Kyriakis, who notes that a broad reading of article 46C (2) is slanted towards the 'organisational approach' to corporate criminal liability. [157] This is because the principal criterion of imparting liability upon the organisation is determined by policies, culture, and practices rather than the personalities and structures. This clause is inextricably connected to paragraph 3, which grants the court the mandate to attribute the conduct of the organisation to the intrinsic policies surrounding the offence.

Another striking feature is paragraph 5, which provides that criminal liability of legal persons may not absolve their natural accomplices from culpability. In essence, this clause acts as a tool for tearing down the wall of separation between the organisation and the promoters, which enables the court mandate to the imposition of criminal sanctions upon the natural promoters. [158]

11.025 Criminal Sanctions against Corporations

Article 43A outlines the available criminal sanctions for corporate perpetrators in terms of pecuniary fines and forfeiture of any property, proceeds or assets acquired unlawfully or through criminal conduct. In addition, Article 45 states that convicted persons can be ordered to pay reparations to victims in terms of restitution, compensation, and rehabilitation.

Article 46M empowers the court to confiscate any asset that was illicitly acquired and transferred to provide legal aid assistance to benefit the victims.

12.0 Corporate Liability under the Malabo Protocol

The institutional framework of the protocol grants the court universal jurisdiction to handle various forms of corporate criminal liability. For instance, if a corporation dumps hazardous chemical waste in a human settlement, then it may be charged with genocide, crimes against humanity, and environmental degradation.[159] Upon conviction, it may be ordered to pay a fine and reparations

156 Eric, Colvin 'Corporate Personality and Criminal Liability'[1995] Criminal Law Forum 6 (1) 15, 18.
157 Ibid pg. 820.
158 Ibid paragraph 5.
159 Schwegler, Vanessa 'The Disposable Nature: The Case of Ecocide and Corporate Accountability' Summer [2017] Amsterdam Law Forum 72.

to the victims *in tandem* with the directors facing criminal charges.

By and large, Article 46C signifies a great leap forward towards the eradication of corporate impunity in Africa. This is because it offers a clear and definitive path to the prosecution of the myriad offences that may be committed by corporations in Africa. In addition, the fact that this clause is anchored on a robust institutional framework is emblematic of its potential success in realising this objective.

13.0 The Role of Reparations in Ensuring Justice for Victims of Corporate Criminal Liability under the Malabo Protocol

The overriding objective of reparations is to compensate victims for the losses incurred due to the offence in three ways; restitution, compensation, and satisfaction.[160] Restitution intends to reinstate the victims to their position prior to the commission or omission of the offence. Conversely, compensation is monetary payment for quantifiable financial damage that emanates from crime. Finally, satisfaction is inherently non-monetary since it seeks to address the intangible aspects of the violations of human rights suffered by the victims[161]. Examples include admission, apology, undertaking non-repetition of the offence, and assurance to apprehend and punish the perpetrators.

In terms of contemporary international criminal law, this remedy was codified in article 85 of the Rome Statute.[162] In *Thomas Lubanga vs. Prosecutor,* where the Appellate Chambers identified the essential ingredients for this remedy as; identifying the victims as natural persons, evidence of harm or injuries, the crime must fall well within the jurisdiction of the court, and proof of causation between the crime and injury.[163]

In terms of the Malabo Protocol, article 20 provides for the right to reparations for victims of gross violation of human rights.[164] In determining this matter the court will be guided by various principles which include: causation,

160 Emanuela Chiara- Gillard, September 'Reparations for Violations of International Humanitarian Law' [2003] Review of the International Committee of Red Cross 85 (831), 531.

161 Ibid.

162 Anja, Wiersing 'Lubanga and its implications for victims seeking reparations at the International Criminal Court' Summer [2012] Amsterdam Law Forum, 25.

163 *Prosecutor v Thomas Lubanga Dyilo*, Judgement on the Appeals of the Prosecutor and Defence against Trial Chamber 1 Decision on Victims Participation of 18 January 2008, ICC-01/04-01/06-1432, A. Ch. 11 July 2008; See also *The Situation in the Democratic Republic of Congo,* Decision on the application for Participation in Proceedings of VPRS1,VPRS2,VPRS3,VPRS4,VPRS5 and VPRS6, ICC-01/04-101-tEN- Corr, Pre-T Ch. 1, 17 January 2006, 9.

164 Ibid.

standard of proof, the role of the court, and the trust fund for victims. Article 45 (3) empowers the court to make orders on reparations after considering the representation from the convict, victims, and interested persons before making the necessary orders.

To qualify for this remedy the applicant must prove harm, injury, and or loss occasioned upon conviction of the perpetrator.[165] Noteworthy, clause 46M establishes the Trust Fund for the 'legal assistance and benefit for victims of human rights violations and their families.'[166] In part, this clause is instrumental in financing the legal representation of the victims before the court. In retrospect, the *Wiwa* and *Kiobel cases* underscored the multifaceted challenges encountered by victims who pursue corporate entities under the conventional civil litigation system. For instance, the victims were from Nigeria, but they were compelled to incur the financial and logistical burden of traveling to the United States for purposes of instituting the legal proceedings. [167]

In addition, the focus of the special tribunals, either for conflicts in Rwanda or Sierra Leone, was to punish the perpetrators who bore the greatest political responsibilities rather than ensuring payment of reparations to victims. Subsequently, it is fair to infer that, despite the challenges and loopholes, this provision is a significant and positive step towards securing reparations for a victims of corporate criminal activities in Africa. However, as Godfrey Musila notes, the overall success of the court is incumbent upon the cooperation and support of member states or donors.[168]

14.0 Potential Challenges and Possible Solutions

14.1 Piercing the Corporate Veil

Corporations operate as registered companies with limited share capital distributed among the shareholders.[169] This complex structure makes it difficult to impugn the perpetrator because it erects a 'Chinese

165 Ibid.

166 Ibid.

167 Jennifer L. Karnes, 'Pirates Incorporated: *Kiobel vs. Royal Dutch Petroleum Ltd* and the Uncertain State of Corporate Criminal Liability for Human Rights Violation under the Alien Tort Statute, [2012] Buffallo Law Review, 60 (3), 263.

168 Godfrey Musila, 'A Promise Too Dear? The Right to Reparations for Victims of International Crimes Under the Malabo Protocol of the African Criminal Court' in Charles C. Jalloh, Kamari M. Clarke and Vincent O. Nmehielle, *The African Court of Justice and Human and People's Rights in Context: Development and Challenges*, 947, Cambridge [2017].

169 *Salomon vs. Salomon & Co. Ltd*. [1894] UKHL 1.

wall' separating the entity from the owners.[170] However, this rule is not absolute since this veil can be pierced when preferring criminal charges against a corporation.[171] Furthermore, abiding by this rule would encourage natural offenders to enshroud their criminal ventures behind the veil of corporations, as stated in the Nuremberg tribunal:-

"Crimes against international law are committed by men, not abstract entities, and only by punishing individuals who commit such crimes can the provisions of international law be enforced."[172]

Thirdly, there should be consistency when enforcing international criminal law.[173] As Ronald Slye cogently argues, if the veil of national sovereignty is lifted and political leaders are prosecuted by international criminal tribunals, why can't corporations be held to the same standard?[174]

This legal conundrum resurfaced at the Special Tribunal for Lebanon (STL) in the *SAL & Al Khayat* cases.[175] The defendants were cited for contempt after broadcasting the details of confidential prosecution witnesses who were placed under the protection program.[176] Nonetheless, they successfully raised a preliminary objection challenging the tribunal's jurisdiction over corporate entities.[177] Upon appeal by the prosecution, the decision was overruled, and the matter was referred back to trial court for the full hearing.[178] The appellate judges held that the word 'person' espoused both legal and natural persons.

Upon full hearing of the matter, the court reaffirmed its decision since the appellate decision was merely persuasive for lack of unanimity

170 Olivier, De Schutter 'Towards a New Treaty on Business and Human Rights' [2016] Business and Human Rights Journal 1 (1), 48.

171 Helen Anderson 'Piercing the Veil on Corporate Groups in Australia: The Case for Reforms' [2009] Melbourne University Law Review 33, 335.

172 International Military Tribunal (Nuremberg). Judgement and Sentences 1st October 1946.

173 Engle, Karen 'Anti Impunity and the Turn to Criminal Law in Human Rights' [2015] Cornell Law Review 100, 1070.

174 Slye, C. Ronald 'Corporations, Veils and International Criminal Liability' [2008] Brooklyn Journal of International Law 33 (3) 957.

175 *Prosecutor v Al Jadeed* S.A.L & Al Khayat STL-14-05/1/CJ 31st January 2014 and Akhbar Beirut & Ibrahim Mohamed Al Amin (STL-14-06/1/Pres) 31st January 2014.

176 Under Rule 60 of the Statute the Court is empowered to hold any person who knowingly and willfully interferes with its administration of justice.

177 *Prosecutor v Al Jadeed S.A.L & Al Khayat* STL-14-05/1/CJ delivered on the 24th of July 2014.

178 *New S.A.L. and Karma Mohamed Tahsin al Khayat,* STL 14-05/PT/AP/ARI26.1 Delivered on the 2nd of October 2014.

among the judges.[179] Furthermore, the inanimate existence of *stare decisis* in international criminal law hampered the court's ability to determine the issue exhaustively. However, the prosecution appealed the ruling, which was allowed on the same previous grounds and referred to the trial court.[180] Despite the constant back and forth, this was a landmark decision since Nuremberg, where an international criminal tribunal exerted its jurisdiction over a corporate body.[181] Subsequently, it offers a persuasive argument for international criminal courts to prosecute corporations for their actions.[182]

Thirdly, the court may improvise the *vicarious liability theory* to hold the principal organisation culpable for the actions of the servants or agents while performing their duty. This theory is anchored on three essential requirements: the commission or omission of the offence, occurrence within the scope of employment, and for the benefit of the principal.[183]

Alternatively, the *identification/alter ego theory* integrates the employee with the business entity thereby creating a bipartite relationship between the corporation and third parties which in turn will hold the corporation liable for the actions of its employee.[184] Unlike vicarious liability, there is no need for delegation since the principle requirement is commission of an offence by an employee for the ultimate benefit of the corporation. However, this school of thought is restricted to the upper echelons of the Organisation, which may obscure the identity of the offenders, especially in conglomerates.[185]

179 *Akhbar Beirut & Ibrahim Mohamed Al Amin* (STL-14-06/1/PT/CJ) delivered on the 6th November 2014.

180 *Akhbar Beirut S.A.L. and Ibrahim Mohamed Al-Amin* (STL-14-06/PT/AP/AR126.1) delivered on the 23rd of January 2015.

181 Kaeb, Caroline 'The Shifting Sands over corporate criminal liability under International criminal law'[2016] George Washington University International Law Review 49, 364.

182 Bernaz, Nadia 'Corporate Criminal Liability under International Law the New TV A.S.A.L. and Akhbar Cases at the Special Tribunal for Lebanon'(2015) Journal of International Criminal Justice 13, 329.

183 *Mousell Brothers Ltd vs. London & Northwester Railway Co. Ltd*. [1917] 2 KB 836; *New York Central & Hudson River Railroad Co. v US*. 212 US 481 (1909).

184 *DPP v Kent & Sussex Contractors Ltd* [1944] KB 146.

185 Yarosky, Harvey 'The Criminal Liability of Corporations' McGill Law Journal 10 (2) 145.

15.0 Prospects and Challenges of Ratification of the Malabo Protocol by the Member States of the African Union

Noteworthy, there is legitimate concern that the inordinate delay if member states ratify the protocol will frustrate the establishment of this court. As Abass notes, African states are 'notoriously quick' to adopt treaties but 'excruciatingly slow' to ratify them.[186] With specific reference to the Malabo protocol, he notes this hesitance stems from the vested interests of African leaders regarding economic and political crimes. For instance, in 2012, the Heads of State summit referred the draft protocol to the AU Court for the interpretation of the words 'corruption' and 'unconstitutional change of government'. This lethargy illustrates how the leaders frowned upon the court for fear of being indicted for economic and political crimes, which are prevalent across the continent.

In the same vein, it is cogent to argue the Malabo protocol is a 'protest treaty' that was conceived by African states to counter the Rome Statute. As Abass points out such treatise are usually driven by 'momentary desires' rather than genuine concern to address the underlying legal issues.[187] Ultimately, the commitment to enforce will wither away once the emotional outburst and or perceived threat begins to dissipate. For instance, when the ICC withdrew the cases against President Uhuru Kenyatta and his Deputy William Ruto, it further contributed to the delay in ratification of the treaty since the AU Heads of State had accomplished their mission to protect their members.[188]

The fourth reason behind this delay is article 46 of the Statute which grants the court complementary jurisdiction together with other regional courts. In essence, the continent is balkanised into four major regions: North, West, South, and East & Central each with regional courts. Against the backdrop of this geographical framework most leaders have their loyalty divided between the regional and continental courts thereby decelerating the ratification process.[189]

Finally, the court is a complex organisation which will require significant resources to realise its objectives as a credible and functional continental

186 Adeniola Abass 'The Proposed International Criminal Jurisdiction for the African Court: Some Problematic Aspects' [2013] Netherlands International Law Review, LX 37.

187 Ibid at pg 42.

188 *Prosecutor v Uhuru Muigai Kenyatta* ICC-01/09-02/11 & *Prosecutor v. William Samoei Ruto* ICC-01/09-01/11.

189 Ademola, Abass 'Prosecuting International Crimes in Africa: Rationale Prospects and Challenges' [2013] European Journal of International Law, 24 (3).

criminal court.[190] However, most African states suffer from financial constraints due to the underdeveloped nature of their economies.[191] Consequently, the long-term going concern of the court is at risk since the funding is anchored on volatile and undeveloped economies if not foreign financing. From another viewpoint, the ruling elite fear if the court is susceptible to foreign financing, then it will morph into a perfect trojan horse for foreign interests to control African affairs.

16.0 The question of jurisdiction over foreign corporations

There is foreseeable risk that foreign corporations may challenge the jurisdiction of the African court.[192] Nonetheless, this concern is addressed by the fact that the mandate is couched in broad and mandatory terms to accommodate contravention of human rights as envisaged by the charter.[193] This overriding objective is equally enunciated by article 28 (h), which stipulates the court shall determine disputes on the nature or extent of the reparation to be made for breach of an international obligation.'

Similarly, this issue may be tackled by viewing international criminal offences through the lens of *jus cogens.*[194] This approach is echoed by article 31 (1) (c) of the protocol recognises customary international law as a source of law. This means the legal obligation to protect human rights is too sacrosanct to be shirked by any entity, including corporations.[195]This principle was substantiated in the *Furundzija case*, where the ICTY stated:

> *"One of the consequences of jus cogens character bestowed by the international community upon the prohibition of torture is that every state is entitled to investigate, prosecute and punish or to extradite the suspect to another competent state."*[196]

190 Stuart, Ford 'Between Hope and Doubt: The Malabo Protocol and the Resource Requirements of an African Criminal Court' in Charles C. Jalloh, Kamari M. Clarke and Vincent O. Nmehielle, *The African Court of Justice and Human and People's Rights in Context: Development and Challenges,* 1077, Cambridge [2019].

191 Vincent O. Nmehielle 'Financing and Sustaining The African Court of Justice Human and People's Rights in Charles C. Jalloh, Kamari M. Clarke and Vincent O. Nmehielle, *The African Court of Justice and Human and People's Rights in Context: Development and Challenges,* 1077, Cambridge [2019].

192 DeGuzman, M. Margret 'Gravity and the Legitimacy of the International Criminal Court' [2008] Fordham International Law Journal 32 (5), 1410.

193 Ibid. Article 28 of the Statute.

194 Ibid Article 53 of the Vienna Convention on the Laws of Treatise; Zgonec-Rozec, Misa and Foakes, Joanne 2013 'International Criminals: Extradite or Prosecute' July Chatham House International Law 4.

195 Hossain, Kamrul 'The Obligation of Jus Cogens and Obligation under the UN Charter' [2005] Santa Clara Journal of International Law 3 (1), 74.

196 *Prosecutor v Furundzija* Case No, IT-95-17/1-T Judgement Trial Chamber, 10 December 1998, Para

In summary, the grotesque nature of international criminal offences should be a sufficient reason for the court to exert its jurisdiction over foreign corporations.

17.0 The Implication of the Executive Immunity Clause on the Efficacy of the Court

By dint of Article 46A, all chief executives and senior government officials shall be granted immunity from prosecution during their tenure in office. This, by far, is the most controversial, problematic, and divisive clause in the protocol since it contradicts the legal principle of equality before the law.[197] This legal principle was succinctly reiterated by the appeals chamber of the special court for Sierra Leone in *Prosecutor v Charles Taylor,* which observed: -

> *"The principle seems now established that the sovereign equality of states does not prevent a Head of State from being prosecuted before an international tribunal or court."*[198]

As Adam Branch notes, the court has been criticised as an 'ineffective and compromised' institution that will shield political leaders from criminal responsibility.[199] Consequently, there is legitimate concern whether the AU is committed to end impunity in Africa.[200] More often than not, corporations connive with political leaders in subverting the rule of law. Therefore, exonerating political perpetrators will break the chain of transactions within the criminal enterprise, thereby impeding the prosecution of corporate accomplices .[201]

Secondly, this clause absolves the state from its primary obligation of preventing violations of human rights by private entities, including corporations.[202] The

156.

197 Netsanet Belay and Japhet Biegon, 'Civil Society and International Criminal Justice in Africa: Perspectives on the Proposed African Court of Justice and Human Rights' in Charles C. Jalloh, Kamari M. Clarke and Vincent O. Nmehielle, *The African Court of Justice and Human and People's Rights in Context: Development and Challenges*, 1113, Cambridge [2019].

198 *Prosecutor v Charles Ghankay Taylor* Case Number SCSL 2003-10 Appeals Chamber, Decision on Immunity from Jurisdiction 31 May 2004 at paragraph 52.

199 Adam Branch, 'African Criminal Court: Towards an Emancipatory Politics' in Charles C. Jalloh, Kamari M. Clarke and Vincent O. Nmehielle (Eds) *The African Court of Justice and Human and Peoples' in Context Development and Challenges Cambridge*, (2009), 200-202.

200 Gartha Abraham 'Africa's Evolving Continental Court Structures: At the Crossroads? Governance and OPRM' January (2015) Program Occasional Paper 209, 14.

201 Amnesty International, 'Malabo Protocol; Legal and Institutional Implications of the Merged and Expanded Court' 2016, 27.

202 Chirwa, Mzikenge Danwood 'The Doctrine of State Responsibility as a Potential Means of Holding Private State Actors Accountable to Human Rights' [2004] Melbourne Journal of International Law 5, 27.

President, being the guardian of the Constitution has the primary duty to protect the rights and dignity of the people. In essence, this clause besmirches the credibility of the court, and it should be revisited and repealed to uphold the rule of law in Africa.

18.0 Conclusion

In conclusion, there is a need for African countries to address the crimes that are committed by corporations. However, as discussed, the enforcement of Article 46 C of the Malabo Protocol will be a remarkable step towards the prosecution of corporations for violation of human rights in Africa.[203] However, it would be prudent to exercise cautious optimism on the success of the court since it is still at the stage of conception. Furthermore, there is a strong likelihood the court will be encumbered with a myriad of obligations which would turn laborious and costly in the long run.[204] Despite these foreseeable challenges there it is fair surmise that the establishment of the court will play a crucial role in addressing this concern.

203 Kyriakakis, Joanna 'Corporate Criminal Liability at the African Criminal Court' -Briefing Paper-ACRI Meeting, Arusha 1 September 2016 at 1 available at http://www.africancourtresearch.com/wp-content/uploads/2016/07/Kyriakakis_Briefing-Paper_-ACRI-2016-Meeting.pdf (accessed on 15 December 2017).

204 Du Plessis, Max 'Implications of the AU decision to give the African Court jurisdiction over international crimes' June (2012) Security Studies Institute for Security Studies 7.

KCB BANK

KCB Multicurrency Prepaid Card

18 Currencies, 1 Card

Apply for your KCB Multicurrency Prepaid Card today and save on exchange rates.

KES | USD | EUR | GBP | AUD | CAD | CNY | INR | AED

CHF | ZAR | JPY | TZS | UGX | RWF | NOK | DKK | SEK

For People. For Better.

Regulated by the Central Bank of Kenya

Civil Society Organizations as Champions of Reproductive Health Rights and Policy Programming in Kenya

Lorian Mona[1*]

Abstract

This article examines the role of Civil Society Organizations (CSOs) in shaping Sexual and Reproductive Health and Rights (SRHR) policies and programs in Kenya. Drawing on a review of existing literature, online SRHR platforms, and data from training sessions led by key CSOs, the study analyzes their contributions to advancing SRHR and identifies persisting gaps in documentation and practice. Focus group discussions with experts, youth, and legal advocates complement the desk review to provide a comprehensive understanding of CSOs' influence. Findings indicate that CSOs have played a pivotal role in promoting inclusive, accessible, and participatory reproductive health services, advancing reproductive justice, and influencing legal and policy reforms. However, systemic barriers continue to hinder progress, including resistance from cultural, religious, and political actors, as well as insufficient institutional and technical capacity, weak policy frameworks, inadequate healthcare infrastructure, and limited funding. Additional challenges, such as poverty, stigma, and harmful cultural norms, further restrict access to SRHR information and services. The study concludes that CSOs are essential in bridging policy and implementation gaps by countering misinformation, delivering services, expanding access to SRHR information, and mobilizing stakeholders to uphold reproductive rights. Strengthening the institutional and financial capacity of CSOs and fostering collaboration with government and international partners are crucial for sustaining advocacy and ensuring equitable access to comprehensive SRHR, particularly for marginalized populations amid rising anti-rights opposition.

Keywords: *Anti-rights actors*, *Civil Society Organization*, *Policy programming*, *Reproductive Justice*, *Sexual and Reproductive Health and Rights*

1 * Lorian Mona is an Advocate of the High Court of Kenya and holds an LLB from Moi University. She is the Founder of Lorian & Co. Advocates, where she specializes in constitutional law, governance, employment and labour relations, human rights litigation and general legal practice. A member of the Law Society of Kenya, she has contributed to several human rights publications and is an active advocate for social justice and good governance.

1.0 Introduction

Reproductive health policies in Kenya should be geared towards the achievement of the highest attainable standards of health, and toward the achievement of each person's highest potential as consistent with the provisions of Article 19(2) of the Constitution of Kenya.[2] Likewise, reproductive health policy in Kenya should take into account global commitments regarding reproductive justice and toward education, especially for young girls, and boys as agreed at the 1994 International Conference on Population and Development and outlined in the Programme of Action of the International Conference on Population and Development including; gender equity and equality; infant, child and maternal mortality reduction; and the provision of universal access to quality reproductive health services, such as family planning, abortion and sexual and reproductive health information for all persons of reproductive age- and with further special attention to Articles 2(5) and 2(6) which brings international agreed to treaties and customary international law within the purview of national law in Kenya.[3]

And yet, national commitments often do not reflect this desired reality, nor aim to attain these national and international commitments, and either display a laissez-faire attitude towards their practical achievement or in the worst-case scenario, an attitude of opposition towards the achievement of these goals. This is especially the case, where budgetary commitments in Kenya keep falling below the recommended 15 percent pledged in the Abuja Declaration, and showing little specificity towards demonstrating the practical steps aimed towards advancing reproductive health.[4]

2 The *Constitution of Kenya*, 2010, Article 19 (2) the purpose of recognizing and protecting human rights and fundamental freedoms is to preserve the dignity of individuals and communities and to promote social justice and the realization of the full potential of all human beings

3 Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW); International Covenant on Civil and Political Rights (ICCPR); Programme of Action of the International Conference on Population and Development adopted at the International Conference on Population and Development Cairo, 5–13 September 1994; the Beijing Declaration and Platform for Action 1995; the African Charter on the Rights and Welfare of the Child (ACRWC) and the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa

4 Republic of Kenya. 2024 Budget Policy Statement, Sustaining Bottom-Up Economic Transformation Agenda for Economic Recovery and Improved Livelihoods. February 2024 SRHR issues were the most raised issues in the health sector during public participation in F/Y 24/25. In F/Y 2025/2026, only 3.2 per cent of the budget was allocated to healthcare; The Abuja Declaration on HIV/AIDS, Tuberculosis and other infectious diseases, African Summit on HIV/AIDS, Tuberculosis and other related infectious diseases, Abuja, Nigeria April 24-27, 2001 In April 2001 Heads of State of the African Union made a commitment to allocate at least 15% of their annual national budgets to the health sector

Having committed to the Programme of Action adopted in Cairo in 1974, Kenya has since taken several steps, including the adoption of a constitutional right to the highest attainable standard of health, including reproductive health, under Article 43(1)[5] ultimately, leading to the enactment of the Health Act in 2017, and related sexual and reproductive health policies, including the National Guidelines for Quality Obstetrics and Perinatal Care, Standards and Guidelines for Reducing Morbidity and Mortality from Unsafe Abortion, 2012: the National Road Map for accelerating the attainment of MDGs related to Maternal and Newborn Health in Kenya. (2008-2015), The National Reproductive Health Policy 2022-2032, among others, resulting in the reduction of maternal and child and infant mortality and better health outcomes overall.

Still, the country falls behind in achieving its mortality reduction goals below 147 per 100,000 live births or in curbing Sexual and Gender Based Violence (SGBV).[6]

Infringements on sexual and reproductive health rights (SRHR) persist, and are much more prevalent by national and local governments as well as private persons and institutions, hence threatening the achievement of equality, dignity, and security of all persons, and the universally recognized human right to health[7]. Oftentimes, these infringements manifest into a reversal of gains in the area of reproductive health, despite existing interventions or overall improvements in reproductive health outcomes. For instance, the withdrawal of the Standards and Guidelines for Reducing Morbidity and Mortality from Unsafe Abortion, 2012 and the subsequent banning of abortion training of medical professionals by the national government left a gap in the provision of access of SRHR services and information, leaving young girls and women susceptible to unsafe abortion, therefore infringing upon both the rights of

5 The Constitution of Kenya, 2010, Article 43 (1) (a)

6 National Council for Population and Development, Division of Family Health, Population Studies and Research Institute (PSRI), Population Reference Bureau. *Reducing Maternal Deaths in Kenya,* Policy Brief No. 46 (June 2015) <https://ncpd.go.ke/wp-content/uploads/2021/02/Policy-Brief-46-Maternal-Deaths-in-Kenya.pdf>

7 Swedish International Development Cooperation Agency (Sida), Sexual and Reproductive Health and Rights, Policy Brief (2011) <https://cdn.sida.se/app/uploads/2021/12/21141349/10205777_Sida_Brief_SRHR_dec-2021_webb.pdf> accessed 10 October 2025 Sexual and Reproductive Health and Rights (SRHR) may be defined as the complete, physical, mental, emotional, psychological, social and spiritual well-being of the person in all matters relating to Sexual health, Sexual Rights, Reproductive health and Reproductive rights regarding all matters comprised of the Reproductive system, its functions, processes, and outputs and the means (including rights and entitlements) with which to achieve these rights or complete state of well-being, and not merely the absence of disease or infirmity, and includes the encompassing right of all individuals to make informed choices about their bodies, sexuality, and reproduction without violence, coercion, or discrimination

young women and girls and medical providers in accessing or providing SRHR and scientific progress related thereto.[8] Infringements are also present in the lack of adequate budgeting and financing of healthcare services, including reproductive healthcare, leading to inadequate capacity and provision and a heightened risk of abuse in reproductive health settings due to a lack of adequate capacity, information, equipment, and trained healthcare professionals.

Recognizing this grim reality, and given the need to ensure that SRHR remain central to national and global policy, Civil Society Organizations (CSOs) have worked to remain at the forefront- holding the State and other institutions, including hospitals, accountable, and in advocating for policies that prioritize access to comprehensive healthcare, inclusive of comprehensive reproductive healthcare services, upholds human rights, and address the diverse needs of the population through evidence-based and participatory initiatives.[9]

The object of this paper is therefore to analyze the contributions by CSOs in promoting reproductive health rights and policies in Kenya. It concludes by finding that while CSOs' contributions to Reproductive Justice is commendable; there is a need to further strengthen and support their capacities, including their technical, political, and financial capacities to ensure their continued participation and effectiveness in the reproductive health policy-shaping and programming process in Kenya.[10]

8 Constitution of Kenya 2010, Fourth Schedule, para 2. Under the Fourth Schedule at Paragraph 2 of the Constitution, the development of health and other policy is the responsibility of the National government while service provision is entrusted to devolved governments; Federation of Women Lawyers (Fida – Kenya) & 3 others v Attorney General & 2 others; East Africa Center for Law & Justice & 6 others (Interested Party) & Women's Link Worldwide & 2 others (Amicus Curiae) [2019] eKLR, High Court at Nairobi, Petition 266 of 2015

9 D Uberoi, T Ojo, A Sriharan and others, 'What can implementation science offer civil society in their efforts to drive rights-based health reform?' (2023) 8 Global Health Research and Policy 1 <https://doi.org/10.1186/s41256-023-00284-4>

10 'What is Reproductive Justice?' <https://www.sistersong.net/reproductive-justice> accessed 10 October 2025. Reproductive justice may be defined as a state of access to justice in all matters regarding reproductive health including the social, cultural, economic and political determinants of reproductive health such as access to information and which accounts for systemic barriers such as poverty, illiteracy, negative socio-cultural norms and practices including stigma and allows for full autonomy and a state of complete physical, emotional and psychological and emotional well-being for all persons in all matters of sexual and reproductive hath. It was coined by women of color (Women of African Descent for Reproductive Justice) in the mid-1990s and seeks to expound on reproductive rights by including social justice concerns

2.0 Anti-rights Groups and Narratives in Kenya and the Role of CSOs in Countering Anti-reproductive rights Narratives

2.01 Overview of anti-rights groups

Considerable progress has been made in realizing reproductive health and rights in Kenya since 1974, but much remains to be made, and especially so where anti-rights groups' actions seek to reverse the gains made in reproductive health policy.[11]

Against this background, anti-rights groups, including anti-gender groups, negatively impact SRHR and reproductive health policy and continue to do so, by perpetuating harmful norms, narratives, and practices that take away from the full enjoyment of sexual and reproductive health and rights and by pursuing political, social, and legal tactics that seek to limit the enjoyment of these rights.[12] While there is no way to categorize anti-rights groups, most anti-rights groups present in the form of religious groups, cultural groups, conservative political movements, or politicians, speaking to the systemic nature of the institutional barriers to SRHR in the form of opposition.[13]

Notwithstanding their presentation, anti-rights action in the context of reproductive health negatively impacts SRHR, especially for the most vulnerable groups and persons, such as poor women, and vulnerable children or young girls and adolescents, resulting in negative, life-threatening outcomes and the deprivation of important SRHR for most people. For example, harmful cultural practices such as female genital mutilation/cutting (fgm/c) which threaten the right to dignity, life, health and freedom of security of victims may be deeply rooted in cultural practices and beliefs and existing in conservative populations-

11 RFSU, SRHR as a Prerequisite for Democratic and Economic Development, Recommendations to the EU and Its Member States (May 2023) <https://www.rfsu.se/globalassets/pdf/srhr-and-development-for-the-eu_230511.pdf> accessed 10 October 2025

12 Rebecca Oas, 'Anti-Rights: The New Censorship Weapon of the Left' Definitions: A Monthly Look at UN Terms and Ideas (14 September 2024) Issue 35, Center for Family and Human Rights (C-Fam) <https://c-fam.org/wp-content/uploads/Definitions-Anti-Rights.pdf> accessed 10 October 2025. Anti-rights actors and groups may be defined as actors who actively campaign and work against the recognition, protection, and advancement of human rights and fundamental freedoms including the police, civil society organizations, the media, religious organizations and elected officials. This can include sexual and reproductive rights. In the context of SRHR, they include opponents of progressive social policies like abortion, comprehensive sexuality education, homosexual marriage, and transgender policies

13 Oas, 'Anti-Rights' (n 7). The unifying feature of such groups is opposition to gender ideology, a framing of women's rights based on the right of a woman to access abortion, homosexual sex and marriage and opposition to ideologically extreme sex education for children

requiring intensive community sensitization and other locally-led initiatives such as alternative ritualistic programmes (arps) to influence behavioural and attitudinal change.[14] Such harmful practices, although drastically reduced, continue to persist and to perpetuate inequality and discrimination in the full enjoyment of reproductive rights of all women and particularly for marginalized women and communities, including the poor.

Opposition may also be presented from conservative religious groups and politicians leveraging religious and moral arguments that deeply appeal to rooted cultural, patriarchal, or religious values, influencing political leaders and policymakers to propose restrictive reproductive healthcare policies and laws or to create negative stigma around important SRHR and SRHR providers and advocates, resulting in a net negative in the enjoyment of the full spectrum of SRHR. [15]

Kenya is reported to have one of the highest burdens of teenage pregnancy globally, increasing the susceptibility of young Kenyan girls to drop out of school, to gender-based violence, poverty and to exploitation.[16] In the same breath, the rates of unsafe abortion are estimated to be about 465,000 a year,[17] posing an understandable cause for concern either from established and influential reproductive justice advocates, conservative and religious groups and the political establishment. In these circumstances, the motivations for anti-rights groups may appear to be geared towards the same objective as human rights groups and civil society organizations. To end teenage pregnancies.

However, anti-rights groups are often non-supportive of comprehensive reproductive health care, and generally oppose comprehensive SRHR

14 P Mwendwa, N Mutea, MJ Kaimuri and others, 'Promote locally led initiatives to fight female genital mutilation/cutting (FGM/C), lessons from anti-FGM/C advocates in rural Kenya' (2020) 17 Reproductive Health 30 <https://doi.org/10.1186/s12978-020-0884-5>

15 Kelvin Mokaya, 'Production and Dissemination of Anti-Rights Rhetoric as Religious Knowledge on Sexuality' (3 July 2024) <https://nayakenya.org/2024/07/03/production-and-dissemination-of-anti-rights-rhetoric-as-religious-knowledge-on-sexuality/> accessed 10 October 2025

16 National Council for Population and Development, UNFPA and African Institute for Development Policy (AFIDEP), 'Teenage pregnancy and motherhood situation in Kenya: the county burden and driving factors; policy brief' (2016)

17 Kenya National Bureau of Statistics (KNBS) and ICF, Kenya Demographic and Health Survey (KDHS) 2022: Volume 1 (2023) KNBS and ICF, Nairobi and Rockville, Maryland. According to the KDHS 2022, 15% of adolescent women aged 15–19 have ever been pregnant: 12% have given birth, 1% have experienced a pregnancy loss, and 3% are pregnant with their first child

which is inclusive of the full spectrum of SRHR services including support for sexual and reproductive well-being, fertility, infertility, access to contraception, abortion, sex education and information relating to the reproductive healthcare, and in the process, seek to limit the right to information and other procedural safeguards needed to achieve the full enjoyment of SRHR [18]

Anti-rights groups also perpetuate misinformation about various aspects of SRHR, including contraception and abortion, Comprehensive Sexuality Education (CSE), amongst others, limiting the public's understanding of reproductive health and rights, and further reinforcing negative and conservative social norms that limit the full access to sexual and reproductive health and services.[19] For instance, anti-rights actors often perpetuate misinformation narratives such as "Abortion is murder" or "Abortion is a crime" or that CSE promotes promiscuity, and frame their opposition to CSE, contraception, and safe abortion as a defense of traditional family structures or religious morality, perpetuating stigma which may negatively influence the seeking of SRHR services.[20]

This risk is exacerbated as anti-rights groups become more emboldened due to increased funding, political support, wins, and other actions that seek to hearten anti-rights narratives. [21] For instance, anti-rights actors in the reproductive rights sector in Kenya including the Kenya Christians Professionals Forum have sought to lodge an Appeal against the High Court decision in, FIDA-Kenya and others v. Attorney General and others Constitutional Petition 266 of 2015, finding that where the life or health of the mother is in danger, including where a victim is a survivor of sexual violence, women and girls have a right

18 C Onwuachi-Saunders, QP Dang and J Murray, 'Reproductive Rights, Reproductive Justice: Redefining Challenges to Create Optimal Health for All Women' (2019) 9(1) Journal of Health Sciences and Humanities 19

19 JN John, S Gorman, D Scales and J Gorman, 'Online Misleading Information About Women's Reproductive Health: A Narrative Review' (2025) 40(5) Journal of General Internal Medicine 1123 <https://doi.org/10.1007/s11606-024-09118-6>

20 'CSOs Explore Strategies to Confront the Criminalization of Sexual and Reproductive Health (SRHR) in Africa' (23 July 2025) <https://www.kelinkenya.org/csos-explore-strategies-to-confront-the-criminalization-of-sexual-and-reproductive-health-srhr-in-africa/> accessed 10 October 2025

21 Neha Wadekar, 'America's Anti-Abortion Business Is Booming in Africa' (2024) <https://www.ipas.org/wp-content/uploads/2024/11/foreignpolicy.com-Americas-Anti-Abortion-Groups-Are-Booming-in-Africa.pdf> accessed 5 October 2025; 'Movement Building' <https://rhnk.org/our-work/movement-building> accessed 5 October 2025

to access Abortion.[22] In the Appeal, and together with the Attorney General, the religious group is seeking the Court of Appeal to find that Abortion is not a constitutional right.[23]

But pro-SRHR CSOs understand that there are less restrictive means to achieve these goals, that would ensure the dignity and security of all persons, including young women, girls, and adolescents, ultimately leading to equity, equality, and inclusion of all persons in reproductive justice outcomes. For instance, by promoting access to information on the right to reproductive health care and rights, CSOs help to tackle anti-reproductive rights narratives and misinformation, and therefore help people and communities to make better, more informed choices to ensure the full realization of all SRHRs for all persons.[24]

3.0 Anti-rights groups and their impact on reproductive health policy

To ensure their objectives are met, anti-rights groups, including religious groups, often employ legal as well as social tools and strategies to formalize their opposition to sexual and reproductive rights, limit access to vital reproductive services, and negatively influence reproductive health and policy-hindering progress toward gender equality and reproductive justice, further resulting in further inequality.[25]

For instance, the National Council of Churches of Kenya (NCCK), a conglomeration of churches opposed to the changes proposed in the Reproductive Health Bill 2019 presented a Memorandum to Kenya's Senate.[26] They argued that its enactment would lead to a degradation of societal values, citing concerns over the proposed abortion, contraception, and sexuality education provisions which they argued would erode the ethical foundations of Kenyan society.[27] To date, the Reproductive Healthcare Bill 2019 has not

22 FIDA–Kenya v Attorney General (n 7)

23 Center for Reproductive Rights, 'Center to Defend Landmark Decision in Kenya Guaranteeing Abortion Access for Survivors of Sexual Violence' (6 October 2025) <https://reproductiverights.org/jmm-fida-appeal-abortion-kenya/> accessed 5 October 2025

24 'The Role of the Media: Promoting Responsible and Inclusive Reporting on SRHR' (23 July 2025) <https://www.kelinkenya.org/the-role-of-the-media-promoting-responsible-and-inclusive-reporting-on-srhr/> accessed 5 October 2025

25 'Hold the Line: Resisting Frontline Attacks on Sexual and Reproductive Health and Rights' (MSI Reproductive Choices, March 2025) <https://www.msichoices.org/wp-content/uploads/2025/03/Hold-the-line-Resisting-frontline-attacks-on-sexual-and-reproductive-health-and-rights-1.pdf> accessed 5 October 2025

26 W Mothata, 'Church, Anti-Abortion Groups Seen Threatening Women's Health Bill in Kenya' (SABC News, 20 September 2020) <https://www.sabcnews.com/sabcnews/church-anti-abortion-groups-seen-threatening-womens-health-bill-in-kenya/>

27 National Council of Churches of Kenya (NCCK), 'Our Presentation to the Senate on High Rates

been enacted. Narratives surrounding its provision for abortion outside the limits of the constitution, CSE, and assisted reproduction failed to reach the necessary consensus or have the necessary buy-in to pass the Bill, with the Ministry of Health (MoH) seeking to have it aligned with existing constitutional provisions and other stakeholder views. [28] Meaning thousands of young women and girls are left without access to essential reproductive healthcare services or reproductive healthcare information, which can be life-threatening.

While, we do not claim that the Bill lags due to the actions of religious groups, their influence cannot be entirely disputed, and speaks to not only an emboldened opposition but also demonstrate how non states actors including religious groups and other anti-rights actors including other CSOSs often influence policy on reproductive health, by erecting legal and administrative barriers to access of reproductive rights.[29]

Further, these attempts at restrictions to access comprehensive SRHR often speak to a wider conservative and political agenda to restrict other rights, including civil and political rights, other rights including cpr such as the right to information and to self-determination, and further highlighting the inter-dependability of all human rights to ensure the full realization of SRHR.

For instance, the Peter Kaluma-sponsored Family Protection Bill sought to restrict the rights of sexual minorities to choose whom to have sex with by seeking to legislate on 'traditional family values', alluding to increased funding from conservative American groups and Christian organizations to local anti-rights groups and politicians in Africa, reportedly.[30] In September 2024, the Kenyan Member of Parliament (MP) caused uproar on social media for intimating that he was in the United States, campaigning for the Trump Presidential Campaign, speaking to emboldened political support for reportedly anti-rights groups and actors.[31]

---

of Teenage Pregnancies' (13 March 2019) <https://www.ncck.org/our-presentation-to-the-senate-on-high-rates-of-teenage-pregnancies/>

28 'Health Ministry Wants Abortion Bill Withdrawn for More Talks' (Business Daily, 11 August 2020) <https://www.businessdailyafrica.com/economy/Health-ministry-wants-abortion-bill-withdrawn-talks/3946234-5607580-y0facz/index.html> accessed 10 October 2025

29 Wadekar, 'America's Anti-Abortion Business' (n 20)

30 'Kenya on the Verge of Tabling Anti-LGBTQ Bill in Parliament' (Africa News, 18 July 2023) <https://www.africanews.com/2023/07/18/kenya-on-the-verge-of-tabling-anti-lgbtq-bill-in-parliament/> accessed 11 August 2024

31 P Kaluma [@gpdkaluma], 'Just arrived in New York to campaign for @realDonaldTrump and Republicans. We are Pro-God, Pro-Family, Pro-Life. God Bless USA. God Bless the World' (X, 4 September 2024) <https://x.com/gpdkaluma/status/1831358249930473576?t=3NfHDRAabbXPPry_hzxL-g&s=03>; Wadekar, 'America's Anti-Abortion Business' (n 20) reporting that there had been increased funding to

Given their emboldened action, increased funding and increased political support, retrogressive actions from anti-rights groups then require organized and strategic, legal, political and social interventions from other non-state actors including civil society organizations, non-governmental organizations (NGOs), professional associations such as the Law Society of Kenya to preserve the human rights of all persons, including women and young girls, including women and young girls, and the right to reproductive health care.[32]

4.0 Strategies employed by CSOs to counter anti-rights narratives

In contrast to anti-rights groups' actions, which negatively impact on reproductive health policy and rights, pro-reproductive health NGOs and CSOs often employ different strategies to counter anti-reproductive rights narratives.

These strategies include, engaging in political advocacy, lobbying for policy and legislation, partnerships, including with governments and other CSOs and NGOs, advocating for financing of comprehensive reproductive healthcare services, the use of traditional and non-traditional media to provide information on reproductive health, the employment of new technologies and tools including artificial intelligence to promote SRHR, community mobilization, the use of champions of reproductive health services to support peer to peer advocacy, support of reproductive justice initiatives such as strategic litigation, offering pro bono legal representation to victims of violations of SRHR, evidence based initiatives, provision of healthcare services, among others.[33]

4.01 Interventions– community sensitization/mobilization, and training

One way in which CSOs work to counter anti-rights narratives is by tackling misinformation, especially through their advocacy initiatives, community sensitizations, and mobilization programs, and trainings that seek to provide comprehensive information on reproductive health and sexuality education. This leads to improve and increase access to information needed to fully realize the right to health, including

Africa from "U.S. Christian Right organizations" and that "many of the groups named in the report have close ties to former President Donald Trump and his administration and have influenced Trump on reproductive rights issues."

32 E Opondo, J Maina and N Munyasia, 'Lessons from Kenya on Sexual Reproductive Health and Rights Policymaking: The Need to Centre Voices from Africa in Global Discourses' (2024) 32(1) Sexual and Reproductive Health Matters 2409548 <https://www.tandfonline.com/doi/pdf/10.1080/26410397.2024.2409548>

33 'Movement Building' (n 20), noting that RHNK was established in 2010 as an association of trained healthcare providers under the Society's Act and uses strategies such as lobbying, activist training, strategic litigation, and public awareness campaigns

reproductive health.[34]

For instance, the Reproductive Health Network of Kenya (RHNK) engages in targeted initiatives such as community outreach, static clinics, and sensitization programs, including in marginalized areas in Samburu, Isiolo, and Kajiado, to ensure that SRHR information is able to reach even the most marginalized areas.[35] Their interventions also include training for different professionals and groups that are culturally and norms-sensitive as well as Values Clarification and Attitude Transformation (VCAT) and advocacy training in areas such as the legal framework and abortion, and post abortion care.[36]

Such initiatives by CSOs such as RHNK are usually aimed at everyone in society, including medical professionals and healthcare providers, community counsellors, community health promoters (CHPs), legal professionals, teachers and parents, and young men, women, girls, boys, and adolescents.[37] RHNK also partners with the government, including the Ministry of Health (MoH), in awareness and sensitization training and during the policy-making process in reproductive health matters, including public participation[38].

34 Leonard Cheshire, 'Community Engagement for Inclusive Sexual and Reproductive Health: A Guide for Conducting Workshops with Persons with Disabilities' (December 2020) <https://www.leonardcheshire.org/sites/default/files/2021-11/Community-engagement-inclusive-sexual-reproductive-health.pdf> accessed 18 August 2025

35 Reproductive Health Network Kenya [@rhnkorg], 'Today, we're offering FREE family planning consultations and services across 3 counties—Samburu, Bungoma, and Isiolo—at 4 different facilities (Swipe to see the different locations). Swing by and take advantage! Don't forget to spread the word—tell a friend to tell a friend! Let's make sure everyone has access to the family planning and contraception services they need' (X, 28 August 2024) <https://x.com/rhnkorg/status/1828695946382770189?t=8o1iD9pzfGhZ6yWOXMOzBQ&s=19>

36 Reproductive Health Network Kenya, 'Annual Report 2023' <https://rhnk.org/documents/RHNK-2023-Annual-Report.pdf> accessed 27 November 2025

37 F Kerubo and I Indeje, 'Revolutionizing access to sexual and reproductive health information and service in Kenya through digital health initiatives' (RHNK, November 2024) <https://blog.rhnk.org/revolutionizing-access-to-sexual-and-reproductive-health-information-and-service-in-kenya-through-digital-health-initiatives/> accessed 27 November 2025

38 Maryanne W Waweru, 'The Contribution of IPPF's Partner Organization in Kenya in the Country's Population Programmes' (IPPF Africa Blog, 5 September 2024) <https://africa.ippf.org/blogs/contribution-ippfs-partner-organization-kenya-countrys-population-programmes> accessed 27 November 2025, noting that together with other CSOs and stakeholders, RHNK supported the DRMH in the development of the Kenya Reproductive, Maternal, Newborn, Child, and Adolescent Health (RMNCAH) Policy (2017–2030), the Clinical Handbook on the Prevention and Management of the BIG 5 Direct Causes of Maternal Morbidity and Mortality in Kenya, the National Guideline on Mifepristone and Misoprostol Combination (combi-pack), the National Guidelines for Self-Care in Reproductive Health, and the Kenya DMPA-SC Costed Implementation Plan (2024–2030), among others

The aim for such grassroots interventions and organizing is to listen to the voices of everyone involved in the reproductive healthcare ecosystem and to account for their needs, realities, and barriers in accessing SRHR, providing services, and or advocating for SRHR, and particularly to ensure that formulation, implementation, and evaluation of policy is evidence-based[39].

4.02 Improving access to SRHR services and information

For instance, by conducting training to medical professionals on their duties, rights and responsibilities for example, on the place of conscientious objections and how they can be done within the law, referrals and the right to emergency treatment, there is improved access to reproductive healthcare and information including essential abortion healthcare services, where a trained medical professional might have opted to invoke religious justifications for refusal to offer abortion care services without this training or information.

4.03 Reproductive Justice initiatives, including Promoting Access to Justice for Victims of violations of SRHR

Together with its partners, RHNK and other local and international NGOs such as the International Planned Parenthood Federation (IPPF)(African Region(IPPFAR), the Center for Reproductive Rights (CRR), and the Kenya Ethical and Legal Issues Network (KELIN) also conduct training of legal professionals and collaborate with practitioners in the justice sector to ensure they can be better placed to serve reproductive justice initiatives. [40] This includes *pro bono* representation of victims of violations of SRHR and medical professionals in court and strategic and public interest litigation that translate into policy pronouncements, such as the place of reproductive rights within the Bill of Rights, or interventions such as structural interdicts.[41] Lawyers and legal professionals are also exposed to VCAT

39 J M Zulu, I Goicolea, J Kinsman, I F Sandøy, A Blystad, C Mulubwa, M C Makasa, C Michelo, P Musonda and A-K Hurtig, 'Community based interventions for strengthening adolescent sexual reproductive health and rights: how can they be integrated and sustained? A realist evaluation protocol from Zambia' (2018) 15(1) Reproductive Health 145 <https://doi.org/10.1186/s12978-018-0590-8> accessed 27 November 2025.

40 Reproductive Health Network Kenya, 'About Us: Member Associations' (International Planned Parenthood Federation, 7 September 2024) <https://www.ippf.org/about-us/member-associations/reproductive-health-network-kenya> accessed 27 November 2025

41 In Constitutional Petition 266 of 2015, while it did not result in a structural interdict, the Constitutional Court directed the Kenyan Parliament to enact a law on abortion and post abortion care that was consistent with Article 26(4) and other statutory instruments and policy documents

training to better advance legal representation, access to justice, and reproductive justice goals, given the diverse backgrounds from which professionals in the ecosystem are pooled.[42]

4.04 Inclusive and Participatory Interventions

RHNK conducts training for parents and teachers so that they can understand the reproductive rights of young persons and their obligations under the law.[43] For instance, parents and guardians must understand the place of consent in obtaining crucial SRHR for young persons under their direction, given parental privilege granted by the law, whilst understanding that teenagers are deserving of their own autonomy.[44]

CSOs also engage in training aimed at adolescents to ensure that they can understand their rights in SRHR and to make empowered decisions about their reproductive health. Youth and adolescents training on SRHR recognize their vulnerable state while balancing the legal responsibility of care, control, and imparting values left to parents and guardians, while also acknowledging their bodily autonomy and the right to make informed decisions about their sexual and reproductive lives and access justice regarding the same.[45] For instance, in the city of Kisumu, the risks of teenage pregnancy are high on the agenda for the Network for Adolescent and Youth of Africa (NAYA), an organization that offers support and advice to young people across a whole range of issues, including reproductive and sexual health, and sexuality through

allowing for safe and legal abortion and care: FIDA–Kenya (n 7); Daniel Ng'etich & 2 others v Attorney General & 3 others [2016] eKLR (Petition No 329 of 2014, High Court of Kenya at Nairobi, Mumbi Ngugi J, 24 March 2016), while this adjudication did not specifically deal with SRHR, KELIN, an NGO registered under the Non-Governmental Organization Co-ordination Act No 19 of 1990 and committed to the protection, promotion and enhancement of enjoyment of the right to health through public interest litigation, advocacy and law reform, together with other NGOs including the National Empowerment Network of People living with HIV/AIDS in Kenya (NEPHAK) and the AIDS Law Project, was able to secure reliefs in the nature of structural interdicts to ensure policy measures against the involuntary confinement of persons with TB and other infectious diseases

42 Reproductive Health Network Kenya, 'Spreading compassion, and initiating change' <https://rhnk.org/our-work> accessed 15 August 2024

43 Reproductive Health Network Kenya, 'Addressing the THREE ZEROS by Prioritizing Adolescents & Young People's SRHR' in 4th RHNK Annual Scientific Conference on Youth and Adolescent SRHR, AYSRHR Conference Abstract Booklet (2020) <https://rhnk.org/documents/abstracts/4th-RNHK-AYSRHR-Conference_Abstract-Booklet.pdf> accessed 15 August 2024

44 Health Act, No. 21 of 2017 ; Children's Act, No. 29 of 2022

45 Women's Global Network for Reproductive Rights Africa, 'Youth Sexual and Reproductive Health and Rights (SRHR) Training Toolkit' (19 June 2022) <https://wgnrrafrica.org/youth-sexual-and-reproductive-health-and-rights-srhr-training-toolkit/> accessed 15 August 2024

a participatory Advocacy Model for the Youth.[46]

These actions lead to strategic partnerships and alliances with other NGOs that reflect the needs and aspirations of all members of society.[47] By listening to the voices of those closest to the ground, guiding them to make empowered decisions, and ensuring that programming, including in policy making, is relevant, sensitive, and attuned to the community's needs and cultural norms, these CSOs serve an important function in bringing important SRHR closer to the people and communities.

5.0 Successful Counteractions within Reproductive Justice

In working to protect essential SRHR in Kenya, CSOs have, through innovative and community-centered strategies and initiatives, successfully influenced public opinion and, directly and indirectly, policy outcomes. This section argues that by engaging in innovative forms of advocacy, informed by community interactions, these organizations continue to effectively counter opposition and to create environments that are conducive to progressive policy shifts in reproductive healthcare matters.

For instance, given the rise of digital technologies, CSOs have sought to leverage new and existing technologies such as hotlines and Artificial Intelligence (AI) to improve access to SRHR services and information.

5.01 Case Study 1: The 'Aunty Jane Hotline'

The Aunty Jane Hotline, provided by the Trust for Indigenous Culture and Health (TICAH), [48] provides a service connecting young Kenyan women to open and non-judgmental counselors who provide accurate, confidential, life-saving information on contraception, safe abortion, and sexual health. In the Kenyan context, where misinformation is rampant, systemic and structural, and access to reproductive services, including for young girls, is limited due to stigma and restrictive laws, this initiative directly challenges anti-rights narratives by ensuring women and girls have access to reliable, confidential advice, hence

46 K Mokaya, 'Negation of sexual and reproductive health and rights by anti-rights and anti-gender groups' (Network for Adolescent and Youth of Africa (NAYA), September 2023) <https://nayakenya.org/negation-of-sexual-and-reproductive-health-and-rights-by-anti-rights-and-anti-gender-groups/> accessed 15 August 2024

47 Leonard Cheshire, 'Community engagement for inclusive sexual and reproductive health' (n 33)

48 Trust for Indigenous Culture and Health (TICAH), 'Kenya: Trust for Indigenous Culture and Health' (Women Help Women) <https://womenhelp.org/en/page/413/kenya-trust-for-indigenous-culture-and-health-ticah> accessed 1 September 2024

directly countering harmful and incorrect information propagated by anti-rights groups. By providing reproductive health information safely and anonymously, including safe and legal abortion, the Aunty Jane Hotline not only protects and advances women's rights, including the privacy rights, but also demonstrates how digital tools can be employed to overcome physical, social, and cultural barriers to accessing SRHR. [49]

While the hotline itself is not a policy tool, its success in providing critical services and information has catalyzed discussions around the need for a more robust public health response to SRHR issues, especially for marginalized women and young girls.[50] The existence of such initiatives also influences the direction that primary actors, such as the Kenyan government, can take in implementing health and fiscal policies, including digital health.[51]

5.02 Case Study 2: Kisumu's Teenage Pregnancy Programs

Kisumu County grapples with high rate of teenage pregnancies in Kenya. The African Youth Advocacy Network (AYAN) Kenya has launched various programs in Kisumu and neighboring counties, including Migori and Siaya, targeting young girls and their communities to raise awareness about SRHR. AYAN's initiative involves engaging local leaders and communities, sensitizing them on the dangers of early pregnancies, and offering young girls information on sexual health.[52]

This grassroots approach has countered conservative narratives that often blame teenage pregnancies solely on individual irresponsibility rather than on systemic issues such as poor access to contraception, lack of comprehensive sexual education and other harmful cultural practices and norms. [53]

49 S Norris, 'How a community-run helpline is helping women access safe abortion advice in Kenya' (The Ferret) <https://theferret.scot/aunty-jane-kenya-helpline-access-safe-abortion/> accessed 13 August 2024

50 J Njagi, 'A qualitative approach to interrogating the age and gender divide in digital SRHR platforms in Kenya' (2023) 31(4) Sexual and Reproductive Health Matters 2291908 <https://doi.org/10.1080/26410397.2023.2291908>

51 K Maichuhie, 'The mobile apps keeping adolescents from HIV, pregnancies' The Daily Nation (Nairobi, 20 August 2024) <https://nation.africa/kenya/news/gender/the-mobile-apps-keeping-adolescents-from-hiv-pregnancies-4730810> accessed 27 November 2025

52 AYAN Kenya, 'We Are Because I Am (WABIA Project) – Homabay, Migori, and Kisumu Counties' (2023) <https://ayankenya.org/we-are-because-i-am-wabia-project/> accessed 27 November 2025

53 AYAN Kenya, 'Organization Profile' (2023) <https://ayankenya.org/wp-content/uploads/2023/03/Ayan-profile-2-2.pdf> accessed 27 November 2025

Through partnerships with other CSOs, including TICAH, local schools, and healthcare providers, AYAN has worked to normalize discussions on reproductive health in historically conservative and patriarchal communities, in culturally sensitive ways, making a significant impact in reproductive health programming by ensuring it is participatory.[54] Although it may not yet have been translated into major policy reforms, AYAN's efforts have helped to shape local health programming, demonstrating that cultural resistance can be effectively navigated with community engagement.[55]

5.03 Case Study 3: The Reproductive Health Network of Kenya's 'Nena na Binti' Initiative

Another successful counteraction to improve access to comprehensive SRHR services and information includes the *Nena na Binti* initiative by the Reproductive Health Network of Kenya (RHNK) through its Nena na Binti platform and toll-free line/services. The initiative utilizes trained counselors to offer information and guidance to women and girls utilizing digital tools [56]. RHNK also seeks to leverage technology, including telemedicine, to break the barriers in accessing comprehensive SRHR services and information and especially for underserved communities, through its digital initiatives. By leveraging artificial intelligence and real-time counseling services, the initiative can offer up-to-date SRHR education, contraceptive information, and safe abortion referrals, filling the gap left by inadequate government services.[57] As a result, RHNK's work has started influencing discussions at the policy level, prompting stakeholders to explore how technology and youth can be integrated into Kenya's broader reproductive health framework.[58]

54 AYAN Kenya, 'Intergenerational Dialogue in Kisumu County – Bridging the Gap for SRHR Justice' (Facebook, 25 July 2024) <https://web.facebook.com/africanyouthadvocacynetwork/posts/751537210591652/?_rdc=1&_rdr> accessed 27 November 2025, on 25 July 2024, AYAN Kenya, supported by partner TICAH, hosted an Intergenerational Dialogue between young people, parents, and community leaders in Kisumu County to discuss abortion, stigma, evidence-based and rights-based SRHR, and shared and informed decision-making in SRHR

55 AYAN Kenya, 'Strategic Plan 2023–2026' (August 2023) <https://ayankenya.org/wp-content/uploads/2023/03/AYAN-Strategic-Plan-2023-2026.pdf> accessed 27 November 2025

56 International Campaign for Women's Right to Safe Abortion, 'National Abortion Information Hotlines' (2024) <https://www.safeabortionwomensright.org/i-need-an-abortion/national-abortion-information-hotlines/> accessed 27 November 2025

57 NenaNaBinti, 'Your Confidential, Non-Judgemental SRHR Support' <https://nenanabinti.org/> accessed 5 September 2024

58 Maryanne W Waweru, 'The Contribution of IPPF's Partner Organization in Kenya in the Country's Population Programmes' (n 37)

6.0 Influence of CSO-counteractions on reproductive health rights and policy

The successes of these strategies, initiatives, and counteractions demonstrate how CSOs use available tools, including recent technology, to combat misinformation and improve access to SRHR information and services. By utilizing innovative, participatory, inclusive, and tech-driven strategies, CSOs demonstrate their adaptability in countering anti-rights narratives, especially in underserved areas and in an increasingly modern world.

While these initiatives may not directly drive legislative changes, they do create fertile ground for progressive policy shifts by acting as testing grounds for new technology and policy by setting new precedents for SRHR access and provision, and challenging harmful socio-cultural narratives and norms. For instance, digital health initiatives sought to be implemented by the State may include SRHR services, drawing precedent from CSOs' counteractions, thereby revealing how CSOs' work at the grassroots level may translate into broader public health conversations and set the stage for future policy developments.[59]

7.0 CSOs Judicial Strategies and Contribution to Legal Jurisprudence in Reproductive Rights and Policy

The grassroots momentum connects to the broader influence of CSOs in shaping legal precedents by lodging important court claims on behalf of victims or for the benefit of the public. Demonstrably, these have translated into impactful legal wins that impact SRHR policy in Kenya.

By pursuing redress and access to justice for victims of violations of reproductive rights and lodging public interest and strategic litigation that impact reproductive health policy, CSOs in Kenya have been at the forefront of positively impacting reproductive health rights and policy and broadening the reach of reproductive justice in Kenya.

Jurisprudence influenced by CSOs in Kenyan courts has, for instance, clarified the normative scope of reproductive rights, including clarifying abortion as essential healthcare and as a human rights,[60] clarified obligations for policy makers and those implementing policy, such as local governments, county governments, and other institutions, including Parliament,[61] allowed

59 *ibid*

60 PAK and Salim Mohammed v Attorney General and 3 others [2022] eKLR (Malindi High Court Petition No E009 of 2020, 24 March 2022, R Nyakundi J)

61 JOO (also known as JM) v Attorney General & 4 others [2017] eKLR (Petition No 5 of 2014) while the Court did not find a violation of the Petitioner's right to information, it noted that hospitals may need to put in place complaint mechanisms in order to improve service delivery and handle complaints from the public public to allow for redress in the case of threatened violations

for reprieve or remedies for victims of violations of reproductive rights,[62] held government and institutions accountable, among others, ultimately contributing to the development of national and regional jurisprudence and influencing reproductive health policy.

7.01 The JOO Case: The Role of CSOs in Pursuing Access to Justice for Victims of Violations of Reproductive Rights

Despite the promulgation of a new Constitution on the 27th of August 2010, guaranteeing the highest attainable standards of health, including reproductive health care, and a presidential directive directing the provision of free maternal healthcare services in all public hospitals,[63] one Josephine Oundo Ogwen (JOO) walked into the resident Bungoma County Referral Hospital in August of 2013 in labour, seeking to deliver her pregnancy, but was met with one of the worst cases of abuse and lack of acceptable minimum standards in the healthcare facility.

While at the hospital's maternity ward, there were no beds. JOO was forced to share a bed with another expectant woman. Further ill-equipped, and despite presidential directives and policy on free maternal healthcare, the county hospital at Bungoma forced her to buy her own induction medicine and cotton wool. As she labored on, none of the nurses on duty came in to monitor her progress during labour, and she was forced to give birth on the floor unassisted. When the nurses found that she had begun her delivery on the floor, they verbally and physically abused JOO, forcing her to walk unassisted to the delivery room to complete her already traumatic delivery.

Local and international NGOs, led by the Center for Reproductive Rights (the Center or CRR), took the matter up to the Kenyan High Court on behalf of the Petitioner, claiming violation of her constitutional rights as well as international human rights law.[64] The Center sued the County Government of Bungoma, the Bungoma County Executive Member in charge of health, the Cabinet Secretary of the Ministry of Health, the Bungoma County Referral Hospital, the public hospital where the ill-fated events took place, and the Attorney General of the Republic of Kenya, being the principal legal advisor to the government.

62 FIDA–Kenya v Attorney General (n 7); JOO v Attorney General [2017] eKLR. (n 60)
63 JOO v Attorney General [2017] eKLR (n60)
64 Constitutional of Kenya,2010 Article 2(5) and 2(6)

The Petitioner claimed that, due to the lack of adequate personnel, infrastructure, medical supplies and equipment at the public Bungoma County Referral Hospital, and the neglect and physical and emotional abuse metered to her by medical staff, this constituted a violation of her rights to health, right to dignity, and the right to be free from cruel, inhumane and degrading treatment. The Petitioner also claimed that her right not to be subjected to indiscriminate treatment was violated. She argued that the mistreatment further threatened her right to life by exposing her "to a heightened yet preventable risk of dying during or post-delivery, further exacerbated by the "rampant, systemic and widespread abuse, neglect and mistreatment of pregnant women in Kenya during delivery and post-natal healthcare."[65]

The Court found that in the instance case, the Respondents had violated the Petitioners' right to access quality reproductive health care, and especially so where the Petitioner and other poor women were required to purchase necessities in a public facility, where quality healthcare was anchored in the Constitution and where a Presidential directive provided for free maternal care. This was nothing short of a violation of her human rights.[66] The Court faulted the County Government of Bungoma for its failure to allocate and devote adequate resources to ensure quality reproductive health care. The Court found that in failing to implement, monitor, or provide minimum acceptable standards of health care, and failing to ensure that maternal healthcare services are dignified, this constituted violations by the devolved government of its constitutional obligations to ensure that the highest attainable standards of health are achieved.

The Court also found that the manner in which the Petitioner was made to give birth, and in the most gruesome of ways, on the floor, with no bed, no hospital inputs, or physical or psychological support from nurses who aggravated the situation by abuse and neglect of the Petitioner, violated her rights to dignity and security.

The Court ruled that both the National and County Governments had failed to establish policy guidelines to implement the directives on free maternal care, and that they had further failed to devote

65 Center for Reproductive Rights, 'Abuse and Disrespect, Human Rights Violations in Maternal Health Settings: Fact Sheet' (2018)

66 JOO v Attorney General [2017] eKLR. (n 60)

adequate resources required to implement, monitor, and provide the minimum acceptable standards of healthcare including as provided under international law.[67]

This decision contains implications for National governments who are tasked with establishing policy as well as for County Governments who implement health policy in Kenya, including for budgeting and funding of healthcare and reproductive healthcare services.[68]

The decision also has implications for organizational policies for healthcare facilities, whether private or public, to be able to allow for proper complaints and redress mechanisms .

The filing and ultimate conduct of the petition speak to the role of CSOs, as champions of reproductive health and policy, and in clarifying obligations for the State under local and international law and other actors, and in broadening the normative and operative framework through which Reproductive health rights are viewed and through which policy should necessarily be implemented.

The JOO Case also speaks to the role of CSOs and other NGOs in providing checks and balances to the State, and in holding public and government institutions accountable, including on systemic injustices such as institutional negligence in maternal health care, abuse of pregnant women during delivery and in post-natal health care, and lack of adequate funding and infrastructural support, which exacerbate infant and maternal mortality. ,[69] Ultimately, it also speaks to the role of CSOs and NGOs in helping victims of violations of human rights to pursue justice, including in reproductive healthcare and maternal health settings.

67 Constitution of Kenya, Articles 2(5) and 2 (6) See, The Convention on Elimination on all forms of Discrimination Against Women , 1973 Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa

68 Constitution of Kenya, 2010, The Fourth Schedule

69 ESCR-Net, 'Case Law | Health (Right to) J.M. v Attorney General and 6 others' (14 May 2019) <https://www.escr-net.org/caselaw/2019/jm-v-attorney-general-and-6-others/> accessed 27 November 2025.

7.02 The JMM Case: Safe and legal Abortion and Access to Justice for Victims of Sexual Violence, and CSO's fight against retrogressive implementation of policy

JMM died in 2018, a victim of sexual violence, at only 18 years of age.[70] Following abuse and defilement by an older man at only 14 years of age, she contracted a pregnancy, and staying with an older relative, she did not tell anyone about the pregnancy for fear of being judged and stigmatized. Instead, JMM shared the news of her pregnancy with an older girl and on the 8th December 2014, was introduced to a 'doctor', who "advised" that she could terminate her pregnancy. The so-called doctor invited JMM to a backroom, and without conducting any prior examination, asked her to lie on a bed and injected an unidentified substance into her thigh. She was advised to wait for the fetus to be expelled the next day. When the fetus was not expelled, JMM returned to the pharmacy. The doctor inserted a metal-like cold into her uterus, and she was assured that the fetus would be expelled by evening.

Unbeknownst to her, JMM had undergone an unsafe abortion. Following the 'procedure,' JMM developed complications including severe stomach pain, vomiting, and heavy bleeding. She was taken to the Ibeno dispensary, where preliminary enquiries confirmed the same. However, the dispensary lacked the necessary infrastructure, equipment or necessary facility or staff to offer the required standard of care, and she was referred to Kisii Teaching and Referral Hospital, a Level 5 Hospital, 15.6 km away. She was required to cover the financial costs. About Kshs 12,500 which her mother did not have. She developed kidney problems due to the procedure and complications following it. However, the first hospital she was referred to did not have dialysis services. She was then required to visit Tenwek Mission Hospital, situated in Bomet County, about 50 kilometers from Kisii Town.[71] On the 12th of December 2014, JMM was admitted into the intensive care unit, upon payment of Kshs 3,000.00. At the time of her admission at Tenwek Hospital, JMM was not able to talk. However, while she stayed here for 7 days, and was stabilized, Tenwek Hospital did not have any equipment to undertake dialysis. Her mother, and next friend, PKM, was advised to take JMM either to Moi Teaching and Referral Hospital in Eldoret or Kenyatta National Hospital which

70 FIDA–Kenya v Attorney General (n 7)
71 *ibid*

were all considerable distances away and would come at great financial cost to them.

Tenwek hospital offered the Hospital's ambulance to transport JMM, but only upon her undertaking to settle her hospital bill which had accrued to Kshs 65,000.00 at the time of her discharge. PKM opted to take JMM to Kenyatta National Hospital where they arrived on 19th December 2014 and were immediately admitted for surgical treatment. She continued to receive treatment, including dialysis, until 25th February 2015 when she was discharged as an inpatient but was to continue receiving treatment as an outpatient. At the time of her discharge from Kenyatta National Hospital JMM had had a septic abortion and haemorrhagic shock and developed chronic kidney disease. She was referred for follow-up in the renal unit of Kenyatta National Hospital.[72]

By the time of her discharge, the bill at Kenyatta National Hospital had risen to Kshs. 39,500.00, which PKM was unable to pay. As a result, JMM was detained at the Hospital during which period she slept on a mattress spread on the floor due to the scarcity of beds. She fell sick again during this period of detention and was once again taken to the main ward, where she was treated for about four days. She was then returned to the detention room where she stayed for a period of 2 weeks until her release on 13th March 2015 when the hospital bill was waived. JMM later died from complications shortly following her release.

Local and international NGOs, including The Federation of Women Lawyers in Kenya (FIDA), RHNK, and the Center for Reproductive Rights, sued on behalf of or for the benefit of JMM through her next friend, PKM. They sued the Director of Medical Services (DMS)**,** Ministry of Health (MoH), and the Registrar of the Kenya Medical Practitioners and Dentists Board, the statutory body that regulates the practice of medicine, dentistry, and medical institutions. The Petition was opposed by other non-state actors, including the Kenya Christian Professionals Forum, the Catholic Doctors Association, and the East Africa Center for Law and Justice.

72 *ibid*

The Petitioners argued that the withdrawal of the 2012 Standards and Guidelines and the National Training Curriculum for the Management of Unintended Risk and Unplanned pregnancies as well as the blanket ban on abortion training for healthcare professionals threatened the right to life, under Article 26(1) and (4) and the right to health under Article 43 (1)(a), including reproductive health by creating a lacuna in respect of instances in which abortion is permissible under Kenyan law and with respect to access to abortion, abortion information and post-abortion care and/or emergency treatment. The Petitioners also argued a violation of the right to equality and non-discrimination guaranteed under Article 27, the right to dignity under Article 28, to freedom from cruel, inhuman and degrading treatment guaranteed under Article 29(f) and the right to access information under Article 35(1)(b), as the withdrawal had the effect of depriving the petitioners and other women and girls access to potentially life-saving information and services.[73]

The Court clarified that the right to access quality healthcare, including abortion in certain instances, was guaranteed under Article 26, and especially where, in the opinion of a trained health professional, the life or health of the mother is in danger, including in instances of sexual violence. The Court noted that it was enjoined under the Constitution to consider the social and cultural context within which the claim was made. There was a high incidence of sexual violence among women in Kenya, which disproportionately affected poor women and girls. There was a further high incidence of maternal mortality and morbidity resulting from unsafe abortion, which was further exacerbated by a lack of information on how to access comprehensive SRHR.

It stated that, therefore, Article 26(4) was a compromise that highlighted the instances in which abortion was permissible in Kenya, given its diverse social, religious, and cultural context. Therefore, while abortion was generally not permissible as a rule, the same Constitution provided exceptions to this general rule.

It found that the actions of the *3rd Respondent via* the *letters dated* 3rd December 2013, *and* ***the*** *Memo dated* 24th February 2014, withdrawing the said guidelines, were neither participatory nor inclusive, were unconstitutional, and failed to meet the threshold for violation under Article 24.

73 *ibid*

The lack of policy coordination failed to guide health care professionals on the circumstances in which they could offer abortion and post-abortion care under Kenyan law. The 2014 guidelines also failed to meet the threshold of precision of limitation required under Article 24. The Respondents had violated the Petitioners' *right to the highest attainable standard of health, right to non-discrimination, right to information, consumer rights, and right to benefit from scientific progress as women of reproductive age and other women and adolescent girls of reproductive age.* The Court also found that the state had violated the national values and principles of governance under Article 10 and the right to fair administrative action under Article 47 of the Constitution, including the Fair Administrative Action Act, found their actions and/or omissions *unlawful, illegal, arbitrary, unconstitutional, and thus null and void ab initio.* The Court further found that the rights of health care professionals, including to information, freedom of expression and association, and the right to benefit from and advance scientific progress, had been infringed. It issued compensation to PKM under Article 23 as indemnification for material and emotional harm in damages of Kshs. 3,000,000/=.[74]

In lodging this Petition, CSOs were able to acquire critical legal pronouncements by the Constitutional High Court on the place of abortion within the Kenyan context. It demonstrates how strategic litigation by CSOs have helped to define the scope of reproductive rights, including the legal position on abortion and post abortion care in Kenya-placing access and provision of comprehensive SRHR within legal and policy framework and standards as well as social and cultural contexts. It further highlighted the barriers that exist in accessing comprehensive SRHR and proper reproductive healthcare including financial and material barriers, lack of adequate policy framework, lack of access to information and a lack of access to trained health professionals.

The litigation was also further able to demonstrate policy gaps and the place of policy in addressing systemic issues of women, young girls, and adolescents including Sexual violence, defilement and rape, and the heightened risk of early, unintended pregnancies and reducing maternal morbidity and mortality for women in Kenya and the place

74 FIDA–Kenya v Attorney General (n 7) delivered full bench on 12th Day of June 2019 by Justices A O Muchelule , M. Ngugi , G V Odunga , L A Achode and J M Mativo

of policy including in accessing quality trained professionals to offer healthcare including reproductive healthcare. The Court noted the role of the State in financing of healthcare, capacity building and overall policy making, implementation and monitoring in reducing barriers to access to proper reproductive healthcare.

7.04 *PAK and Salim Mohammed v. Attorney General and Three Others (Malindi High Court Petition Number E009 of 2020)- CSOs challenging Retrogressive Application of Law and Policy*

Whilst receiving important lifesaving treatment and post-abortion care from a trained and licensed healthcare professional at Chamalo Medical Center following complications from a spontaneous abortion, PAK, together with the medical professional, were accosted by police and arrested. During her forceful arrest, PAK, a minor, who had conceived with another minor, was forced to undergo a forced medical examination at the Kilifi County hospital, without her parents' or guardians' consent. The minor, the 1st petitioner, was later charged with the offence of procuring an abortion contrary to section 159 of the Penal Code. The 2nd Petitioner was charged in Kilifi criminal case number 395 of 2019 with procuring an abortion contrary to section 158 of the Penal Code. The DPP also charged him with the offence of supplying drugs to procure abortion contrary to section 160 of the Penal Code in the alternative. PAK was remanded to juvenile prison for one month and was forced to secure bail, which was eventually provided by the Center for Reproductive Rights and RHNK. Mohammed, the medical professional who offered the lifesaving post abortion care, was detained for one week before posting bail[75].

The Petitioners sought a declaration that forcing PAK and women and girls of reproductive age to undergo medical examination with the intention of charging them for procuring abortion violates their rights to health, privacy, dignity and in her case, the right to a fair hearing, and that the arrest, detention and prosecution of patients seeking post-abortion care services is cruel, inhuman and degrading treatment and a violation of Articles 25 (a), 28, 26(4), 43(1) (a), 43(2) and 50 of the Constitution. The Court found that there was a lacuna to operationalize Article 26(4) of the Constitution of Kenya and that Abortion and post-

75 Center for Reproductive Rights, PAK and Salim Mohammed v Attorney General and 3 others [2022] KEHC (Malindi) Petition No E009 of 2020 <https://reproductiverights.org/case/kenya-constitution-abortion-malindi-pak-salim-mohammed/> accessed 6 September 2024

abortion care and programming should embody the Constitutional principles of dignity, autonomy, equality, and bodily integrity. It lightly touched on the considerations by opposition groups in support of anti-abortion sentiment and opposition to comprehensive SRHR, stating that in an egalitarian society, only constitutional principles would prevail in place of other considerations. It found that the right to privacy was a key component of dignity, health, and SRHR. In the circumstances, arbitrary arrests and prosecutions of persons seeking and offering SRHR violated Articles 43(1) and 28(1). The forced examinations violated Articles 25, the right to life under Article 26(4), Article 28 on dignity, the right to freedom and security of the person under Article 29, and the right to privacy under Article 31. [76]

It noted that the lack of policy continues to impede service delivery and endanger the rights of women and girls and their full enjoyment of the right to health and life. The Court directed the Kenyan Parliament to enact a policy framework on safe and legal abortion in line with the Constitutional provisions on the right to life under Article 26 and including Article 26(4). [77]

The litigation and decision further clarified the role of CSOs in defining abortion as a 'fundamental human right' within the Kenyan legal framework and how CSOs employ strategic litigation to champion law and policy for the benefit of all persons and especially the most marginalized, including young girls and adolescents, poor women, indigent women, and other marginalized persons and communities.

8.0 The role of CSOs in Lobbying and Codifying Legislation

The above jurisprudence demonstrates the role of law and a suitable policy framework in granting access to important SRHR. Where adequate policy is in place, there is a demonstrated need from all stakeholders to ensure its implementation to ensure that it adequately serves the needs of persons and communities. In the circumstances, CSOs play a corresponding role in ensuring lobbying for the codification of law and policies on reproductive health and rights, and in all aspects of SRHR programming.

76 PAK and Salim Mohammed v Attorney General and 3 others [2022] KEHC (Malindi) Petition (n 59) was filed by on behalf of the petitioners by the Center for Reproductive Rights and the Reproductive Health Network of Kenya against the Attorney General, the Director of Public Prosecutions, Inspector General of Police, and the Senior Principal Magistrate Kilifi

77 PAK and Salim Mohammed v Attorney General and 3 others [2022] KEHC (Malindi) Petition (n 59)

Indeed, the Reproductive Health Policy bill 2019, and later of 2022, presented a missed opportunity for CSOs to effectively lobby for a law seeking to put in place a framework that would guarantee or provide a structure for the ending of the triple threat: early and unintended teenage pregnancies, new HIV and AIDS infections, and sexual and gender-based violence. Some stakeholders argued that, for instance, the case on Comprehensive Sexuality Education was not well advanced by lobby groups, even though it was well-provided for in the Bill. [78]

The Reproductive Healthcare Bill also embodied various practical provisions for sex education in schools, assisted reproduction, including surrogacy, and access to safe abortion services when necessary[79]. However, the Bill never came to pass because of strong opposition to abortion and comprehensive sexuality provisions and a divergence of views between stakeholders, highlighting the opportunities presented and missed in the enactment of the Reproductive Healthcare Bill, 2019, even as acknowledged by the Constitutional Court in the PAK decision.[80]

There remains much political advocacy and lobbying work to do, as thousands of young girls, adolescents and women continue to be left without adequate SRHR and information, in the absence of an adequate legal and policy framework as intimated by the Constitution under Articles 19(2) and 21(2) of the Constitution, and as found by different Courts of law in the PAK and JMM decisions.[81]

As illustrated through the breadth of CSOs have been central to the policymaking and shaping process, including through the monitoring, evaluation, and enforcement of existing policies and strategic litigation leading to important landmark adjudications in the Court that dictate how policy should be implemented under the current legal and social framework.

78 Laila Le Guen, 'In Kenya, abortion focus obscures legislation towards safe reproductive healthcare services' (Global Voices, 30 March 2021) <https://globalvoices.org/2021/03/30/in-kenya-abortion-campaigners-obscure-legislation-towards-safe-reproductive-healthcare-services/> accessed 27 November 2025.

79 Nita Bhalla, 'Church, anti-abortion groups seen threatening women's health bill in Kenya' (Thomson Reuters Foundation News, 18 September 2020) <https://news.trust.org/item/20200918153131-onhir> accessed 27 November 2025

80 PAK and Salim Mohammed v Attorney General and 3 others [2022] KEHC (Malindi) Petition (n 59)

81 Constitution of Kenya, art 21(2) and art 19(2) The Constitution obliges the State to take legislative, policy and other measures, including setting standards, to progressively realize the rights guaranteed under Article 43, while affirming that the recognition and protection of human rights and fundamental freedoms serve to preserve dignity, promote social justice, and enable the realization of human potential

However, it is important that in adjudicating and advocating for any policy, including in reproductive health care, it should be reflective of the needs, experiences, and aspirations of people and communities, and effectively address their barriers and limitations in accessing comprehensive SRHR. It is not enough to just influence policy, but the process of influencing said policy must be participatory and inclusive of all stakeholders, and the content of such policy must reflect their needs. Indeed, the whole tiff with anti-right groups is that their influence on policy is directed in a manner that is exclusive and not people-centered, but centered on outside, extrinsic goals and selfish motivations.

CSOs serve the function of bridging the gap between people and political entities that often enact or propose policies and laws including in reproductive health care, ensuring that policies are reflective of constitutional aspirations foundational to the full achievement of all human rights and the full potential of all human beings in Kenya and to ensure that the content and implementation of said policy is comprehensive and able to benefit all persons.

8.01 Methods used by CSOs to ensure inclusive policy-making processes

In the bid to ensure that reproductive health policy and programming is inclusive and participatory, CSOs such as The Network for Adolescent and Youth of Africa (NAYA), AYAN and RHNK employ different evidence-based strategies to ensure that they can collect and utilize only the most accurate information to be able to effectively advocate for policy These methods include trainings where experts provide or present evidence-based research, the use of focus groups for purposes of data collection and evaluation, participatory and collaborative ventures such as conferences where evidence and data are presented and analyzed with different stakeholders. [82] For instance, NAYA is a youth led regional advocacy network founded by the African Regional Office of the Planned Parenthood Federation of America (PPFA) in October 2001 that works to improve the technical capacity of youth advocates, young people, youth led organizations and policy makers to undertake SRHR advocacy at international, regional, national and counties in Kenya to improve SRHR quality, affordability, accessibility and information. It uses the Participatory Advocacy Model for the Youth (PAMY) to allow for meaningful youth participation and involvement of young people in its program management cycle.[83]

82 RFSU, 'SRHR as a Prerequisite for Democratic and Economic Development: Recommendations to the EU and Its Member States' (n 10)

83 'NAYA Profile' (NAYA Kenya) <https://nayakenya.org/who-we-are/> accessed 27 November 2025

Other participatory and inclusive interventions include community engagement workshops with different interest groups, including young girls or adolescents, or persons with disabilities. For instance, RHNK, together with sponsors and partners such as IPPFAR and CRR, hosts an annual adolescent youth conference on SRHR where participants can offer real-life evidence-based insights to partner CSOs. The Ministry of Health also participated in the youth and adolescent conference as a co-convener.[84]

8.02 Lessons from successful participatory initiatives: Strategies for successful lobbying and policy advocacy

NGOs such as the Center for Reproductive Rights and RHNK have contributed to the visibility and progress of women's health by engaging in political advocacy, judicial strategies, inclusive participatory processes, advocating for funding appropriations, and demanding increased and improved reproductive health programming.

Given the reported increased opposition to SRHR and opposing views with other stakeholders, including anti-rights actors towards their achievement and realization, CSOs need strengthened and improved technical and financial capacity to improve their effectiveness to lobby and advocate for life-changing policy and legislation.

Accordingly, CSOs can employ different strategies from lessons learnt in their interactions to ensure that they have the renewed capacity needed to deal with emboldened opposition successfully. Borrowing lessons from previous CSO interactions, these strategies can include, collaboration networking, and alliance building, including with other CSOs and NGOs, allowing for skills and technology transfer and exchange, increased technical capacity which would require increased support and funding, a non-adversarial approach to partnerships with the government and political actors to improve the political good will necessary and needed to push important SRHR policy forward, public engagement and grassroots organizing, evidence-based advocacy and documentation, judicial strategies and the employment of international and regional accountability mechanisms and engagements.[85]

84 '7th RHNK Adolescent and Youth Sexual and Reproductive Health and Rights (AYSRHR) Scientific Conference' (PMNCH, 18 June 2024) <https://pmnch.who.int/news-and-events/events/item/2024/06/18/default-calendar/7th-rhnk-adolescent-and-youth-sexual-and-reproductive-health-and-rights-(aysrhr)-scientific-conference> accessed 27 November 2025

85 'Civil Society Organizations (CSOs)' (County Government Toolkit) <https://countytoolkit.

9.0 Conclusion and Recommendations

In conclusion, the impact of CSOs in shaping reproductive health rights and policy in Kenya cannot be gainsaid. Despite facing significant opposition from anti-rights groups and political establishments, CSOs have made substantial contributions to policy development and to legal jurisprudence in reproductive health and rights.

Demonstrably, CSOs have been able to fight retrogressive policy, reinstate good policy that was done away with or not implemented, clarify the scope of reproductive rights and obligations for institutions in the reproductive health policy ecosystem, driving the creation of jurisprudence in reproductive health, driving reproductive health policy towards international standards, keeping the government to account for outright violations of SRHR, monitoring and recommending changes to policy, monitoring opposition and human rights abuses and pursuing justice for victims, keeping the people informed and therefore creating a culture where they can demand better policy and outcomes , tackling misinformation to eliminate stigma and negative societal attitudes, influencing access to services, and bringing important SRHR services and information closer to the people- thereby ensuring greater access to SRHR and that policy and outcomes in reproductive health are participatory, inclusive and dignified, ultimately leading to better health outcomes.

Challenges from opposition groups and political actors continue to impact the work and ultimately, effectiveness of CSOs in delivering important SRHR to populations. For instance, CSOs in reproductive health now have to grapple with the realities and complexities of tackling misinformation from big advertising corporations such as Meta and Google, who now have the backing of large language models and other artificial intelligence technologies as tools at the disposal of anti-rights groups. [86] Such challenges can work to effectively reduce the impact of CSOs in the representation of all persons, and especially those marginalized and vulnerable, calling for strategies to ensure resilience and to overcome opposition, including consensus building.

To be able to effectively carry out their role as watchdogs, and to continue to hold various levels of government accountable in the area of SRHR and in promoting overall good governance in the reproductive sector, CSOs should consider: [87]

devolution.go.ke/civil-society-organisations> accessed 1 September 2024

86 Associated Press, 'In Much of Africa, Abortion Is Legal but Not Advertised' (VOA News, 7 April 2024) <https://www.voanews.com/a/in-much-of-africa-abortion-is-legal-but-not-advertised-/7556173.html>

87 A Minko, 'The Role of Civil Society in Promoting Good Governance in Africa: Challenges and

1. Mutual beneficial partnerships and alliance-building: Strong and ethical leadership supported by robust organizations with clear visions, missions, capacity, strategic partnerships, and alliances that represent all community members, including collaborations with the private sector, other CSOs, regional and international advocacy groups, and governments. Efforts to build consensus with the opposition can also be pursued.

2. SRHR Action Plan: Employ a Strategic Implementation and Action plan for SRHR initiatives backed with organizational cohesion, utilizing case studies and lessons from successes and failures of previous community and political engagement, workshops, training, sensitizations and programs.[88]

3. Technical, and Financial Capacity and Synergies: Exploring capacity building assistance that includes relationship building, and program implementation that links strategies to national efforts and regional and international efforts including programs, evaluation, training, organizational growth, development and adaptability as well as funding through increased domestic and donor financing.

4. Communication, presence and awareness: Use of traditional and non-traditional media, and other technology including, AI, international support and platforms to seek a wider audience e.g. global audience, such as special sessions of the General Assembly to raise awareness, promote research, exchange ideas, benchmark, tackle misinformation and advocate for and influence important national policy, laws and budgets in SRHR that is able to reach and serve populations. Utilizing digital technology and tools to break geographical and social barriers to access of SRHR services and information.

5. Political and policy support for SRHR: Nurture political good will, including in containing anti-SRHR actors as success in SRHR policy is dependent on mainstreaming population needs with national development priorities., by involving decision makers in CSO initiatives and goals, offer trainings and sensitizations to decision makers on SRHR, attuned to their duties, goals and objectives e.g. advocate for integration of SRH interventions into primary health care, universal healthcare and digital health initiatives

Opportunities' (June 2023) Governance in Africa: Challenges and Opportunities, Istanbul University – Turkey <https://doi.org/10.47772/IJRISS.2023.70575>

88 Onwuachi-Saunders, Dang and Murray, 'Reproductive Rights, Reproductive Justice: Redefining Challenges to Create Optimal Health for All Women' (n 17)

6. Leave no one behind: Evidence-based movements involving all persons in SRHR policy programme design, implementation and evaluation through inclusive and participatory processes including grassroots mobilizing and political and community engagement including Persons with disabilities; focusing on disability inclusive programming in SRHR, and all other marginalized persons groups, persons and communities, including refugees, collect , disaggregate and utilize data to ensure policy is evidence-based, help overcome their barriers and ensure no one is left behind. [89]

89 Convention on the Rights of Persons with Disabilities (adopted 13 December 2006, entered into force 3 May 2008) 2515 UNTS 3, art 4(3) The UN Convention on the Rights of Persons with Disabilities underscores the importance of including persons with disabilities at all stages of policy development, programme planning, and implementation

THE ADVOCATES BENEVOLENT ASSOCIATION

The Advocates' Benevolent Association is the welfare arm of the Law Society of Kenya whose main objective is to assist distressed members.

Benefits of membership to the Advocates Benevolent Association:

1. Medical assistance capped at KShs. 150,000/=.
2. Last Expenses cover capped at Kshs. 80,000 for annual members & kshs 100,000/= for life members in the event of a member's demise.
3. Education assistance for children of deceased Advocates subject to limits set by the Board of Management.
   - Nursery school – Kshs. 55,000/= per student per academic year
   - Primary school – Kshs. 80,000/= per student per academic year
   - Secondary school – KShs. 80,000/= per student per academic year
   - Tertiary level – KShs. 100,000/= per student per academic year
   - Kenya School of Law – Kshs. 190,000/=
4. Discounted psychological and counseling services offered in partnership with the Counsellors and Psychologists Society of Kenya (CPS-K).
5. Wakili Personal Retirement Benefits Scheme, a formal retirement savings plan for members of the Association and their non-Advocate employees.

aba@lsk.or.ke 0717-595-006 @LSK_ABA The Advocates' Benevolent Association

MEDIA COUNCIL OF KENYA
COMPLAINTS COMMISSION

RESOLVE IT SWIFTLY AND COST-FREE WITH THE MEDIA COMPLAINTS COMMISSION (MCC)

Have you been wronged by the media? Or are you defending press freedom? **The Media Complaints Commission** is your impartial, expert authority for rapid, no-cost resolution of media disputes under Kenyan law.

Who We Are

The MCC is an independent body established under the Media Council Act 2013, dedicated to handling media appeals and resolving disputes with authority and fairness.

Expert Panel: Led by an Advocate of the High Court and supported by six specialists in journalism, law, regulation, business, arts, and social sciences.

What We Handle

- Mediation or adjudication of disputes between the government and media, the public and media, or within the media on ethical matters.
- Ensuring compliance with the highest standards of journalism as outlined in the Code of Conduct for Media Practice, 2025.
- Delivering impartial, swift, and cost-effective resolutions to complaints against journalists and media outlets, without fear or favour.

Why Choose the MCC Over Court?

- **Cost-Free:** No fees for filing or hearings.
- **Swift:** Disputes resolved within 60 days.
- **Specialist Expertise:** In-depth knowledge of media law and ethics.
- **Impactful:** Binding decisions with meaningful remedies.

Powerful Remedies We Can Order

- Published apologies and corrections.
- Replacement or return of confiscated or damaged equipment.
- Fines up to KShs 500,000 for media outlets or KShs 100,000 for journalists.
- Declarations upholding freedom of expression.
- Publication of our decisions.
- Recommendations for journalist suspensions.

File Your Complaint with Ease

- **Orally:** In person or electronically via **www.complaintscommission.or.ke**
- **In Writing:** Contact the Registrar, outlining your case, the harm suffered, and the remedy sought.

Don't Get Mired in Delays.
Secure Justice Swiftly.

CONTACT US: Registrar@mediacouncil.or.ke www.complaintscommission.or.ke

Headquarters: Ground Floor, Britam Centre, Mara/Ragati Road Junction, Upper Hill, P.O. Box 43132-00100 Phone: +254 727 735252, +254 702 558233, +254 702 558234, +254 702 558463 Email: info@mediacouncil.or.ke

Mombasa Office: Ground Floor, Kenya Broadcasting Corporation Building, Sauti House, off Moi Avenue, along Ngonyo Road Phone: +254 11 101 9220-229 Email: mombasa@mediacouncil.or.ke

Kisumu Office: Kenya Broadcasting Corporation offices, Awuor Otiende Road, Milimani Phone: +254 11 101 9230-239 Email: kisumu@mediacouncil.or.ke

Meru Office: 1st Floor, Posta Buildings, Meru Road B6 Phone: +254 11 101 9250-259 Email: meru@mediacouncil.or.ke

Nakuru Office: Section 58 Area Opposite Crater Primary School along Kibwezi Close, 3rd Cate Phone: +254 11 101 9240-249 Email: nakuru@mediacouncil.or.ke

Digital Rights and Data Protection in Kenya: Privacy, Cybersecurity, and the Impact of Big Data

Silvana Wanjiru[1*]

Abstract

Kenya's rapid digital transformation has reshaped almost every aspect of public and private life. Data gathered through smartphones, online platforms, biometric registration, and financial technology now fuels commerce, governance, and social interactions. Big data, characterized by its volume, speed, and diversity, supports this revolution by enabling predictive analytics, automated decision-making, and personalized services.2 However, the same technologies that improve efficiency also create new vulnerabilities: loss of privacy, algorithmic bias, mass surveillance, and cyber threats. This paper examines how the relationship between digital rights, privacy, and data protection in Kenya is evolving, and how the constitutional and legal frameworks address the ethical and legal challenges of big-data governance. It primarily focuses on Article 31 of the Constitution of Kenya 2010, the Data Protection Act 2019 (DPA), and comparisons with regimes like the EU General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA). The study argues that Kenya's system tends to react rather than prevent issues: enforcement is weak, institutions lack capacity, and algorithmic accountability is underdeveloped. Through doctrinal and comparative analysis, the paper highlights ongoing gaps, particularly the lack of mandatory Data Protection Impact Assessments (DPIAs), unclear consent processes, and limited oversight by the Office of the Data Protection Commissioner (ODPC). It concludes that adopting a rights-based, proactive approach integrating transparency, proportionality, and regional harmonization under the Malabo Convention is crucial for Kenya to protect privacy and human dignity while fostering digital innovation.

Keywords: *Digital rights; Big data; Data protection; Privacy; Cybersecurity; Kenya*

1 [*] Silvana Wanjiru Kamau is an Advocate of the High Court of Kenya with eighteen years' experience in corporate and commercial law, data protection, governance, and regulatory compliance. She is the Principal at Silvana & Associates Advocates in Nairobi and a Certified Secretary (CS-K), where she advises corporations, regulated entities, public institutions, and emerging-technology firms on corporate governance, fintech regulation, digital-rights compliance, and risk management.

2 Charles A Khamala 'Digital surveillance and big data: Balancing the rights to privacy and security in Kenya' [2024] African Journal on Privacy & Data Protection 177

1.0 Introduction

The twenty-first century is defined by the ascendancy of data as a critical economic resource. Across the globe, digitalisation has transformed information into a new factor of production, shaping markets, governance, and social relations. Kenya epitomises this global trend. With an internet-penetration rate exceeding 40 million users by 2024[3]and a mobile-subscription density surpassing 120 per cent,[4]the country stands as one of Africa's foremost digital innovators. Platforms such as M-Pesa, Tala, and Branch have embedded data analytics at the core of financial inclusion, while e-government services like eCitizen and Huduma Namba reflect the state's commitment to digital governance.

However, digital expansion has simultaneously exposed users to unprecedented surveillance and data exploitation. The constitutional guarantee of privacy which is enshrined in Article 31 of the *Constitution of Kenya 2010* affirms the right of every person to be protected from arbitrary interference with personal affairs.[5] Yet, the sheer speed and scale of big-data processing, coupled with emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT), have outpaced the state's regulatory capacity. Data subjects frequently remain unaware of how their information is harvested, shared, or repurposed.

The *Data Protection Act 2019* was intended to bridge this gap. Modelled broadly on the *GDPR*, [6] it institutionalised privacy protection and established the *Office of the Data Protection Commissioner (ODPC)* to enforce compliance. Despite these legislative gains, challenges persist. Limited funding constrains the ODPC's effectiveness.[7] awareness among citizens and small enterprises remains low, and overlapping sectoral laws generate fragmentation. The prevailing model remains reactive, only addressing breaches after they occur rather than embedding preventive safeguards.

This article, therefore, explores how Kenya can evolve from procedural compliance to substantive protection of digital rights. It situates Kenya's data-protection journey within a comparative global and African context, drawing lessons from the *GDPR*, *POPIA*, and the *Malabo Convention*. The analysis unfolds in three parts. First, it examines the emergence of big data in Kenya

3 Communications Authority of Kenya, *Sector Statistics Report Q1 2024* (2024)

4 ibid.

5 Constitution of Kenya 2010, art 31

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation) [2016] OJ L119/1

7 Office of the Data Protection Commissioner (Kenya), *Annual Report 2023* (2023)

and its socio-economic implications. Secondly, it analyses the constitutional, statutory, and institutional framework governing data protection. Thirdly, it outlines reform proposals for strengthening Kenya's capacity to manage digital risks.

2.0 The Rise of Big Data in Kenya

2.1 Defining Big Data

Big data denotes datasets so vast and complex that traditional analytical tools cannot efficiently process them.[8] Scholars commonly describe it through the "three Vs": *volume* (sheer size), *velocity* (speed of generation), and *variety* (diverse formats).[9] Increasingly, commentators add two further dimensions, that is *veracity* and *value*, highlighting the need for reliability and economic utility.[10] In the Kenyan context, data is generated continuously from mobile-money transactions, biometric registration, e-commerce, and social-media engagement. The Central Bank of Kenya reported over 1.3 billion mobile-money transactions in 2023,[11] each producing multiple data points: identity, geolocation, and behavioural patterns. Government initiatives such as *Huduma Namba* and the *Integrated Population Registration System (IPRS)* aim to consolidate citizens' information into interoperable databases, facilitating service delivery but also heightening privacy risks.

As Cukier and Mayer-Schönberger observe, big data shifts epistemology itself: decision-making increasingly relies on correlation rather than causation.[12]This analytical shift challenges traditional legal doctrines, which rely on predictability and accountability, by introducing probabilistic governance where decisions about credit, security, or health derive from statistical inference rather than direct evidence.

2.2 Big Data in Kenya's Digital Ecosystem

Kenya's digital ecosystem rests on three pillars: widespread mobile penetration, fintech innovation, and progressive government digitalisation. Telecommunication giantslike Safaricom, Airtel, and Telkom Kenya collect extensive metadata, including call-detail records, browsing histories, and geospatial coordinates. When integrated with

8 Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013) 23

9 ibid

10 Ibid, 28

11 Central Bank of Kenya, *Mobile Money Statistics 2023* (2024)

12 Mayer-Schönberger and Cukier (n 6) 45.

mobile-money systems like M-Pesa, these datasets reveal intimate behavioural profiles. While such analytics enhance service delivery and fraud detection, they also raise acute privacy concerns when used without explicit consent or oversight.

Fintech companies have particularly leveraged data for micro-lending. Digital-credit applications routinely scrape users' contact lists, SMS content, and location data. A 2021 survey by *FSD Kenya* found that over 50 per cent of borrowers were unaware of how their data was being shared with third-party analytics firms.[13] The *Digital Credit Providers Regulations 2022* now require licensing by the Central Bank of Kenya and compliance with the DPA, yet enforcement remains limited.

E-government initiatives also contribute to massive data accumulation. The *eCitizen Portal* hosts records for taxation, licensing, and passport applications. While centralisation improves administrative efficiency, it also concentrates sensitive data, creating single points of failure vulnerable to cyberattack. The *Huduma Namba* litigation illustrates these tensions: the High Court suspended full implementation until an appropriate data-protection framework was enacted.[14]

The health sector represents another frontier of big-data exploitation. Electronic medical-record systems introduced in public hospitals enhance continuity of care but expose patient information to unauthorised access. In 2022, cybersecurity researchers reported breaches in two major Nairobi hospitals, leaking thousands of records online.[15] Such incidents underscore the need for sector-specific data-governance standards.

2.3 Big Data and the Political Economy

The political dimension of big data manifests most visibly in electoral processes. During the 2013 and 2017 general elections, Kenya witnessed unprecedented use of digital analytics for voter segmentation and targeted messaging. Revelations that *Cambridge Analytica* had operated in Kenya hence collecting psychometric data to craft micro-targeted political advertisements sparked global concern.[16] The scandal exemplified "data-driven manipulation," where personal information

13 FSD Kenya, *Digital Credit Monitoring Report 2021* (2021).
14 *Law Society of Kenya v Attorney General & Others* [2021] eKLR.
15 Cyber Security Africa, *Healthcare Data Breach Survey 2022* (2022).
16 Parliament of Kenya, *Report of the ICT Committee on Cambridge Analytica Allegations* (2019).

is weaponised to influence democratic choice.

Beyond elections, political datafication continues through digital surveillance. Law-enforcement agencies deploy facial-recognition cameras and communication-interception tools purportedly for security. However, absent transparent oversight, such technologies risk contravening Article 31 rights. Scholars such as Nyabola argue that Kenya's digital politics remain "analogue in accountability but digital in reach," producing asymmetrical power between citizens and the state.[17]

Economically, big data has become a driver of innovation. Start-ups leverage analytics for logistics, agriculture, and climate forecasting. Nevertheless, the concentration of data ownership within a few corporations creates *information asymmetry*, granting private actors disproportionate influence over markets and behaviour. Without competition-law coordination and data-portability rights, akin to those in Article 20 of the *GDPR*, Kenya risks reproducing global patterns of digital monopolies.

3.0 Legal and Institutional Framework on Data Protection in Kenya

The regulation of big data in Kenya rests upon a multi-layered framework encompassing constitutional guarantees, statutory enactments, and administrative institutions. This section examines each in turn, demonstrating how privacy protection has evolved from abstract constitutional promise to codified regulatory obligation, albeit with continuing implementation gaps.

3.1 Constitutional Foundations

The cornerstone of Kenya's privacy jurisprudence is **Article 31 of the Constitution of Kenya 2010,** which provides that "every person has the right to privacy, which includes the right not to have their person, home or property searched, their possessions seized or information relating to their family or private affairs unnecessarily required or revealed."[18] This provision embeds privacy within the Bill of Rights and aligns Kenya with international human-rights law, particularly **Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 9 of the African Charter on Human**

17 Nanjala Nyabola, *Digital Democracy, Analogue Politics* (Zed Books 2018) 76.

18 *Constitution of Kenya 2010*, Art 31

and Peoples' Rights (ACHPR).[19]

Judicial interpretation has progressively expanded the meaning of privacy to accommodate technological realities. In ***Coalition for Reform and Democracy (CORD) & 2 Others v Republic of Kenya & 10 Others*** [2015] eKLR, the High Court struck down provisions of the *Security Laws (Amendment) Act 2014* that authorised bulk surveillance without judicial warrant, holding that any limitation of Article 31 must satisfy the constitutional test of legality, necessity, and proportionality.[20] The judgment established that the State must demonstrate a rational connection between the surveillance measure and a legitimate aim, and that less intrusive alternatives are unavailable.

Similarly, in ***Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 Others*** [2020] eKLR, the Court restrained the deployment of a Device Management System capable of accessing mobile-subscriber information in real time. The Court reasoned that unconsented data interception violated both Article 31 and the principles of fair administrative action under Article 47.[21] These decisions underscore an emerging judicial recognition that privacy is a precondition for other freedoms—expression, association, and political participation—and that digital surveillance requires explicit statutory authority and oversight.

Kenya's constitutional text therefore provides a robust normative foundation, but constitutional rights require enabling legislation and institutional machinery for practical effect. This function is performed primarily by the *Data Protection Act 2019* and complementary statutes examined below.

3.2 Statutory and Regulatory Framework

The *Data Protection Act 2019 (DPA)* operationalises Article 31 by prescribing detailed principles for lawful data processing. [22]It defines *personal data* broadly to include information relating to an identifiable

19 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (Art 17); African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217 (Art 9)

20 *Coalition for Reform and Democracy (CORD) & 2 Others v Republic of Kenya & 10 Others* [2015] eKLR

21 *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 Others* [2020] eKLR

22 Data Protection Act No 24 of 2019 (Kenya)

natural person and recognises categories of *sensitive personal data*, such as health status, biometric data, and political affiliation.[23] Section 25 articulates six cardinal principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.[24]These echo the *GDPR's* Article 5 framework.[25]

The DPA also creates enforceable rights for data subjects: access, rectification, erasure, restriction of processing, and objection.[26]Section 30 requires controllers to obtain informed, specific, and unambiguous consent prior to processing. However, consent remains problematic in practice. Many digital-lending apps employ *take-it-or-leave-it* terms, undermining the voluntariness required under Section 32. The *Office of the Data Protection Commissioner (ODPC)* has issued guidance stressing that consent must be granular and revocable.[27]

Cross-border data transfer is regulated under Sections 48–49, which prohibit export of personal data to jurisdictions lacking adequate safeguards. Nevertheless, enforcement remains minimal. In 2022, several Kenyan firms transferred customer information to servers located in Singapore and India without ODPC authorisation.[28] The absence of a statutory requirement for *Data Protection Impact Assessments (DPIAs)* further weakens oversight of high-risk processing, such as biometric registration and algorithmic profiling. By contrast, Article 35 of the *GDPR* mandates DPIAs, and Section 71 of South Africa's *POPIA* restricts automated decision-making that produces legal effects.[29]

The DPA interacts with sector-specific statutes. The *Computer Misuse and Cybercrimes Act 2018* criminalises unauthorised access, interception, and interference with data or systems.[30] The *Kenya Information and Communications Act 1998* regulates electronic communication, while the *Central Bank of Kenya (Digital Credit Providers) Regulations*

23 ibid s 2
24 ibid s 25
25 GDPR, art 5
26 Data Protection Act 2019 s 26–29
27 Office of the Data Protection Commissioner (Kenya), *Guidance Note on Consent and Data Sharing* (2022)
28 ODPC, *Annual Report 2023* (2023) 12–14
29 GDPR Art 35; Protection of Personal Information Act 4 of 2013 (South Africa) s 71
30 Computer Misuse and Cybercrimes Act No 5 of 2018 (Kenya)

2022 impose data-protection obligations on lenders. However, these instruments operate in silos, producing fragmented compliance and jurisdictional overlap. Harmonisation—through a comprehensive digital-governance policy—remains an urgent legislative priority.

3.3 Institutional Oversight and Implementation

The *Office of the Data Protection Commissioner (ODPC)*, established under Section 5 of the DPA, is the linchpin of Kenya's privacy architecture. It functions as an independent regulator mandated to oversee registration of data controllers and processors, investigate complaints, issue enforcement notices, and sensitise the public.[31] Its inaugural *Guidance Note on Consent and Data Sharing (2022)* provided practical benchmarks for compliance, drawing inspiration from the *GDPR* and *POPIA*.[32]

Despite these developments, institutional fragility persists. The ODPC's annual budget for 2023/24 was under KSh 600 million—insufficient for nationwide audits or digital-forensics capacity.[33] Staffing shortages and reliance on external consultants have constrained proactive monitoring. Moreover, the office lacks power to impose substantial administrative fines comparable to those available under Article 83 of the *GDPR*, which authorises penalties up to 4 per cent of global annual turnover.[34] Kenyan sanctions are limited to modest monetary penalties and criminal prosecution, both cumbersome to administer.

Public-sector compliance remains particularly weak. Ministries and county governments often cite "national-security" or "public-interest" exemptions without conducting the balancing tests envisaged by Section 51 of the DPA. For instance, during the 2023 national census pilot, data was collected using digital tablets before the ODPC had reviewed the accompanying privacy-impact framework.[35] Civil-society organisations have criticised this pattern of *compliance by exception*, arguing that it erodes confidence in state stewardship of personal information.[36]

31 Data Protection Act 2019 s 5
32 ODPC (n 25)
33 National Treasury of Kenya, *Budget Estimates 2023/24* (2023)
34 GDPR Art 83
35 Kenya National Bureau of Statistics, *Census Pilot Report 2023* (2023)
36 Article 19 Eastern Africa, *Submission on Public Sector Data Compliance* (2023)

The judiciary and academia have complemented the ODPC's efforts by articulating privacy norms through litigation and scholarship. Decisions such as ***Law Society of Kenya v Attorney General & Others*** [2021] eKLR emphasised the need for data-protection assessments before implementing large-scale biometric systems.[37] Academic commentators advocate multi-stakeholder co-regulation, proposing that professional associations develop sectoral codes akin to those approved under Article 40 of the *GDPR*.[38]Such collaborative models could mitigate the ODPC's capacity constraints while promoting industry ownership of privacy standards.

Finally, Kenya's non-ratification of the *African Union Convention on Cyber Security and Personal Data Protection (2014)*—the *Malabo Convention*—has limited regional cooperation.[39] Ratification would align domestic law with continental norms and facilitate cross-border enforcement, especially as data increasingly flows through cloud-based infrastructure spanning multiple jurisdictions. In the absence of such coordination, Kenya risks regulatory isolation and inconsistent protection for citizens whose data traverse regional networks.

In summary, Kenya possesses a commendable legal foundation for data protection but lacks the institutional muscle to operationalise it effectively. Without adequate resources, technical expertise, and regional collaboration, the ODPC's role remains largely declaratory. A shift towards preventive, risk-based supervision anchored in DPIAs, algorithmic transparency and robust sanctioning powers is essential to realise the constitutional promise of digital privacy.

4.0 Risks and Challenges Posed by the Unregulated Use of Big Data

While big data offers immense potential for innovation, its unregulated use poses substantial risks to privacy, fairness, and autonomy. The absence of robust oversight mechanisms enables both state and private actors to collect, analyse, and share personal data without adequate accountability. This section examines the major risks arising from unregulated big-data practices in Kenya including privacy infringement, discrimination, surveillance, manipulation, and lack of transparency—and evaluates their implications for constitutional rights and democratic governance.

37 *Law Society of Kenya v Attorney General & Others* [2021] eKLR

38 Grace Mutung'u, 'Re-imagining Co-Regulation in Kenyan Data Protection' (2023) 5 African Journal of Cyber Policy 77

39 African Union, *Convention on Cyber Security and Personal Data Protection (Malabo Convention)* (2014)

4.1 Privacy Infringement

Privacy lies at the heart of data protection and is among the most vulnerable rights affected by big-data processing.[40] In Kenya, individuals generate personal information continuously through mobile applications, social media, digital-credit platforms, and e-commerce systems.[41] However, weak consent frameworks and limited enforcement capacity render citizens susceptible to unauthorised access and secondary use of their personal information.

The Huduma Namba digital-identity initiative illustrates this concern. The project sought to consolidate citizens' demographic and biometric data into a single identifier intended for service delivery. In *Law Society of Kenya v Attorney General & Others* [2021] eKLR,[42] the High Court held that the rollout could not proceed without a comprehensive regulatory framework to protect personal data and to operationalise Article 31 of the Constitution. The judgment reaffirmed that technological convenience cannot override constitutional privacy guarantees.

Similarly, in *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 Others* [2020] eKLR,[43] the Court restrained the deployment of a Device Management System capable of real-time monitoring of mobile communications. It ruled that such surveillance would constitute an unjustifiable limitation of privacy and fair administrative action.

Unregulated data processing transforms privacy from an individual safeguard into a systemic risk. Without clear boundaries on consent, purpose limitation, and data retention, personal data becomes a commodity freely traded between corporate and governmental entities. As Solove observes, privacy violations are rarely spectacular events but rather 'a slow series of small intrusions that cumulatively undermine dignity'.[44] The commodification of personal information thus threatens not merely confidentiality but also personal autonomy and democratic participation.

40 Anita L. Allen, 'Protecting one's own privacy in a big data economy', Law, Privacy & Technology Commentary Series, [2016] 130 Harvard Law Review Forum, 71

41 Siddique Latif, Adnan Qayyum, Muhammad Usama, Junaid Qadir, Andrej Zwitter and Muhammad Shahzad 'Caveat emptor: the risks of using big data for human development' Leee Technology and Society Magazine, 38(3), 83

42 *Law Society of Kenya v Attorney General & Others* [2021] eKLR

43 *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 Others* [2020] eKLR

44 Daniel J Solove, *Understanding Privacy* (Harvard UP 2008) 24

4.2 Discrimination and Algorithmic Bias

The rise of algorithmic decision-making in finance, healthcare, employment, and education has introduced new forms of discrimination. Big-data models often replicate historical biases embedded within datasets, producing outcomes that appear neutral yet perpetuate inequality. In algorithmic lending for example, despite being a measure meant to reduce face-to-face discrimination,[45] it can also be a source of inadvertent discrimination.[46] This occurs where big data variables are developed in an unobservable manner but used in statistical discrimination to reconstruct the hidden information using observable proxies.[47]

Kenya's digital-lending sector provides a clear example. Many credit-scoring algorithms rely on non-traditional indicators—mobile-usage patterns, airtime purchases, or social-media activity. These proxies frequently disadvantage women, rural populations, and informal-sector workers who possess limited digital footprints. The Office of the Data Protection Commissioner (ODPC) has received numerous complaints against digital lenders for intrusive data mining and discriminatory scoring practices.[48] In 2022 the Central Bank suspended the licences of several digital-credit providers for non-compliance with data-protection standards.

Comparative jurisprudence underscores the seriousness of algorithmic bias. In *State v Loomis* (2016) 881 N W 2d 749 (Wisconsin SC),[49] the court acknowledged that a proprietary risk-assessment algorithm used in sentencing might reproduce racial disparities but nonetheless allowed its limited use. The decision provoked global debate on transparency and due process in automated decision-making. Under Article 22 of the *General Data Protection Regulation (GDPR)*, individuals have the right not to be subject to a decision based solely on automated processing that significantly affects them.[50] Kenya's Data Protection Act 2019 lacks an equivalent safeguard, leaving data subjects without

45 Robert Bartlett, Adair Morse, Richard Stanton & Nancy Wallace 'Consumer lending discrimination in the fintech era', NBER Working Paper Series 25943, June 2019, 3

46 Barocas, S., and A. Selbst 'Big Data's Disparate Impact' [2016] 104 California Law Review 671

47 Robert Bartlett, Adair Morse, Richard Stanton & Nancy Wallace 'Consumer lending discrimination in the fintech era', NBER Working Paper Series 25943, June 2019, 1.

48 Office of the Data Protection Commissioner (ODPC), *Annual Report 2023* (2023) 10–12

49 *State v Loomis* (2016) 881 NW 2d 749 (Wisconsin SC)

50 GDPR art 22

recourse to challenge biased or erroneous algorithmic determinations.

Algorithmic fairness demands transparency, accountability, and human oversight. As Barocas and Selbst argue, addressing bias requires interrogation of data provenance, model design, and institutional context rather than mere technical fixes.[51] Kenya's data-protection regime should therefore incorporate mandatory *Algorithmic Impact Assessments (AIAs)* for high-risk processing, ensuring that machine learning serves inclusion rather than entrenching structural disadvantage.

4.3 Security Risks and Unregulated Surveillance

Large-scale data storage increases vulnerability to cyber-attacks and breaches. Kenya has recorded numerous incidents involving unauthorised access to voter databases, hospital records, and mobile-money systems. In 2017 the Independent Electoral and Boundaries Commission (IEBC) servers were reportedly compromised, exposing sensitive voter data to manipulation claims.[52] Similarly, health-sector databases have suffered ransomware attacks, endangering patients' personal information.

The *Computer Misuse and Cybercrimes Act 2018* criminalises unauthorised access, interception, and interference with data or systems, yet enforcement remains sporadic. The ODPC lacks the technical capacity to conduct forensic investigations or impose deterrent penalties comparable to those under the *GDPR*.

Unregulated surveillance further compounds these risks. In *Coalition for Reform and Democracy (CORD) & 2 Others v Republic of Kenya & 10 Others* [2015] eKLR,[53] the High Court ruled that interception of communication must satisfy the tests of legality, necessity, and proportionality. Despite this precedent, the proliferation of CCTV networks and biometric monitoring in public spaces has outpaced legal safeguards. Nairobi's *Safe City* surveillance project, implemented with Chinese technology partners, collects facial-recognition data without

51 Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' [2016] 104 California Law Review 671

52 Kenya National Commission on Human Rights, *Report on the 2017 General Elections* (2018) 45–46

53 *Coalition for Reform and Democracy (CORD) & 2 Others v Republic of Kenya & 10 Others* [2015] eKLR

clear retention policies or independent oversight.[54] Such initiatives risk transforming Kenya into a surveillance society in which data gathered for security or administrative efficiency is repurposed for political or commercial objectives.

This phenomenon—often termed 'function creep'—violates Section 25 of the *Data Protection Act 2019*, which codifies the principles of purpose limitation and data minimisation.[55] Without stringent oversight, vast troves of personal data collected for identification or service delivery can be weaponised for repression or discriminatory profiling, undermining public trust and constitutional democracy.

4.4 Manipulation and Erosion of Autonomy

Beyond privacy and discrimination, big data enables unprecedented behavioural prediction and influence. Personal data can be exploited to manipulate consumer choices and political opinions, thereby eroding autonomy and informed consent.

The Cambridge Analytica scandal remains the most notorious example. The firm harvested data from millions of Facebook users to construct psychographic profiles that were allegedly used to influence electoral behaviour, including in Kenya's 2013 and 2017 campaigns.[56] Such practices expose how analytics can transform private information into a tool of psychological engineering, subverting the electorate's capacity for rational decision-making.

As Zuboff argues in *The Age of Surveillance Capitalism* (2019), the extraction of behavioural surplus transforms human experience into raw material for prediction and control.[57] Kenya's digital-marketing and political-consultancy industries increasingly deploy similar tactics—micro-targeting voters or consumers based on inferred vulnerabilities. The result is a subtle erosion of autonomy: individuals are nudged and segmented without awareness or consent.

Legal responses remain limited. The *Data Protection Act 2019* addresses consent and fairness but omits explicit prohibitions on

54 Privacy International, *The Safe City Surveillance Programme in Kenya* (2021)

55 Data Protection Act 2019, s 25

56 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica' *The Guardian* (London, 17 March 2018)

57 Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 93

manipulative profiling. Comparative jurisdictions recognise such dangers: the *GDPR* Recital 71 warns against processing that 'evaluates personal aspects relating to a natural person' for predictive purposes without safeguards.[58] Kenya would benefit from introducing statutory provisions regulating behavioural advertising and political micro-targeting, accompanied by mandatory transparency reports from online platforms.

Autonomy is not merely a philosophical ideal but a constitutional value underpinning human dignity and democracy. As the South African Constitutional Court noted in *National Media Ltd v Jooste* [1996] (3) SA 262 (SCA), privacy ensures 'the right to live one's life with minimum interference'.[59] Unchecked data-driven manipulation undermines this right by converting choice into a function of algorithmic inference.

4.5 Lack of Accountability and Transparency

Opaque data-processing systems, particularly those employing artificial intelligence and machine learning, create profound accountability deficits. Data subjects rarely know how their information is collected, analysed, or shared, and even regulators often lack visibility into proprietary algorithms. Big data relies on mostly unnoticed collection of data, where information from user activity and devices is collected and integrated into massive datasets that can predict behaviors and tendencies. These datasets are analyzed using complex, proprietary tools that are hidden behind legal, technical, and commercial barriers.[60] Thus, even as big data claims to make the world more transparent, the methods and mechanisms behind it remain secretive.[61] This is then referred to as the transparency paradox.[62] This lack of visibility is particularly troubling when big data is used to make decisions about individuals without their knowledge or understanding.[63] Despite the fact that secrecy maybe a requirement for national security and even

58 GDPR recital 71

59 *National Media Ltd v Jooste* [1996] (3) SA 262 (SCA)

60 Neil M. Richards & Jonathan H. King 'Three Paradoxes of Big Data' [2013] 41 Stanford Law Review Online, 42

61 Broeders, D. and H. Dijstelbloem 'The datafication of mobility and migration management: The mediating state and its consequences' in I. van der Ploeg and J. Pridmore (eds.), Digitizing identities, London, 2016, Routledge, 299.

62 Neil M. Richards & Jonathan H. King 'Three Paradoxes of Big Data', 42

63 Ibid, 43

trade secrets, it is only decent that involved people are made aware.[64]

Kenya's *Data Protection Act 2019* articulates general principles of fairness and transparency but does not require disclosure of automated-decision logic or the conduct of *Data Protection Impact Assessments (DPIAs)*. By contrast, Article 35 of the *GDPR* mandates DPIAs for high-risk processing, and Section 57 of South Africa's *Protection of Personal Information Act (POPIA)* empowers the regulator to pre-authorise such activities.[65] Without comparable obligations, Kenyan entities operate within a regulatory grey zone.

Judicial commentary in *Law Society of Kenya v Attorney General & Others* [2021] eKLR emphasised Parliament's duty to legislate clear standards for digital-identity systems.[66] Yet, institutional follow-through has been slow, leaving both public and private actors uncertain about compliance expectations. The resulting opacity fuels public mistrust, especially when breaches occur and victims receive no notification or remedy.

Accountability must become a structural component of Kenya's digital future. Mandatory reporting, independent audits, and algorithmic explainability should form part of every data-processing cycle. As Edwards and Veale observe, transparency is not a panacea but an 'enabler of contestation and oversight'.[67] Embedding these values in Kenyan law would transform the ODPC from a reactive complaints body into a proactive governance institution capable of preventing harm before it occurs.

5.0 Comparative Perspectives and Best Practices in Big Data Governance

Kenya's regulatory experience should be interpreted in light of global and regional data-protection models. The *European Union's General Data Protection Regulation (GDPR)*, *South Africa's Protection of Personal Information Act (POPIA)*, and the *African Union's Malabo Convention* provide valuable benchmarks.

5.1 Lessons from the General Data Protection Regulation (GDPR)

The European Union's *General Data Protection Regulation 2016/679 (GDPR)* represents the world's most sophisticated privacy framework. [68] Its key innovation lies in shifting responsibility from individuals to

64 Ibid, 43
65 Protection of Personal Information Act 4 of 2013 (South Africa), s 57
66 *Law Society of Kenya v Attorney General & Others* [2021] eKLR
67 Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a Right to Explanation Is Probably Not the Remedy You Are Looking For' [2017] 16 Duke L & Tech Review, 18.
68 GDPR, Regulation (EU) 2016/679

data controllers through the principle of *accountability*, which requires entities to demonstrate ongoing compliance with the regulation's principles of lawfulness, fairness, transparency, and purpose limitation.[69]

A cornerstone of the GDPR is its risk-based approach. Article 35 mandates *Data Protection Impact Assessments (DPIAs)* for high-risk processing operations, while Article 30 obliges controllers to maintain detailed processing records.[70] This ensures that compliance is proactive rather than complaint-driven. In contrast, Kenya's *Data Protection Act 2019* (DPA) merely encourages good practice and leaves impact assessments discretionary, resulting in inconsistent adoption across sectors.[71]

The *Court of Justice of the European Union (CJEU)* in *Google Spain SL v AEPD and Mario Costeja González* (C-131/12 2014) established the so-called "right to be forgotten," allowing individuals to demand deletion of outdated or irrelevant online information.[72] The decision underscored informational self-determination as a component of human dignity. Kenya's constitutional privacy clause under Article 31 implicitly recognises a similar right but lacks explicit statutory articulation. Incorporating such a right in the DPA would give citizens greater control over their digital identities.

Moreover, the GDPR provides for substantial administrative fines up to 4 per cent of global annual turnover under Article 83.[73] The availability of deterrent sanctions promotes compliance culture and ensures regulators possess real leverage. By contrast, the Office of the Data Protection Commissioner (ODPC) in Kenya can only impose modest penalties, often insufficient to influence corporate behaviour.[74]

Another instructive feature is the requirement for *Data Protection Officers (DPOs)* in public authorities and in entities engaged in large-scale processing.[75] DPOs act as compliance anchors, bridging the gap between corporate governance and regulatory oversight.

69 Ibid, art 5
70 Ibid, arts 30 & 35
71 Data Protection Act 2019, ss 25–29.
72 *Google Spain SL v AEPD and Mario Costeja González* (C-131/12, 2014) EU:C:2014:317
73 GDPR art 83
74 Office of the Data Protection Commissioner (ODPC), *Annual Report 2023* (2023)
75 GDPR art 37

Institutionalising such roles within Kenyan organisations would professionalise privacy management and relieve the ODPC of routine monitoring burdens.

Finally, GDPR jurisprudence emphasises the doctrine of *extraterritoriality*: Article 3 extends the regulation's reach to processors outside the EU who handle EU citizens' data.[76]Kenya could adapt a similar principle to require foreign digital-service providers operating locally such as global social-media and fintech firms—to comply with domestic privacy obligations, thereby preventing "jurisdictional shopping."

5.2 Insights from South Africa's Protection of Personal Information Act (POPIA)

South Africa's *Protection of Personal Information Act 4 of 2013 (POPIA)* offers a contextual African model of rights-based but pragmatic regulation.[77] It codifies eight processing conditions which are accountability, purpose specification, information quality, openness, security safeguards, and data-subject participation. These conditions mirror GDPR principles yet remain sensitive to local economic realities.[78]

POPIA establishes the *Information Regulator*, an independent authority empowered to issue enforcement notices, conduct compliance audits, and impose administrative fines up to ZAR 10 million.[79] The regulator's active intervention in *Information Regulator of South Africa v Department of Justice and Constitutional Development* (2022) following a ransomware breach demonstrated assertive oversight and transparency expectations.[80]

South Africa's approach also integrates proportionality. Small and medium-sized enterprises enjoy simplified compliance obligations, reflecting resource disparities while maintaining accountability.[81] Kenya could adopt similar tiered obligations through sectoral codes of practice approved by the ODPC, ensuring that compliance costs do not stifle innovation among start-ups.

76 Ibid, art 3
77 Protection of Personal Information Act 4 of 2013 (POPIA)
78 Ibid, chs 3–4
79 Ibid, s 109
80 *Information Regulator v Department of Justice and Constitutional Development* (2022) ZAGPPHC 534
81 POPIA, regs 4–5

POPIA requires prior authorisation for cross-border data transfer unless the receiving state offers an equivalent level of protection.[82]Kenya's DPA contains analogous provisions but lacks detailed adequacy criteria, leaving determinations to administrative discretion. Establishing transparent adequacy guidelines would improve predictability for international data flows and foster investor confidence.

Another instructive aspect is POPIA's mandatory *Information Officer* role, functionally similar to the EU DPO, charged with ensuring internal compliance and training.[83] This institutionalises privacy governance within organisations rather than relegating it to periodic external audits.

South Africa's regulator also prioritises public education and collaborative compliance.[84] In 2023, it launched nationwide awareness campaigns and industry roundtables to demystify obligations. Kenya's ODPC, operating with limited funding, could emulate this outreach strategy to build a privacy-conscious culture rather than relying solely on punitive enforcement.

5.3 Regional Framework: The Malabo Convention

At the continental level, the *African Union Convention on Cyber Security and Personal Data Protection (2014)* (the Malabo Convention) provides a normative blueprint for data governance in Africa.[85] Articles 8–14 stipulate fair, lawful, and transparent processing, require establishment of national data-protection authorities, and regulate cross-border data transfer. The Convention further obliges member states to adopt cybersecurity measures compatible with human-rights standards.[86]

Although Kenya signed the Convention in 2014, ratification remains pending.[87] Ratification would harmonise Kenya's DPA with continental norms, facilitate mutual assistance among African regulators, and strengthen enforcement of transnational privacy breaches.[88] This is particularly critical given Kenya's ambition to serve as a regional technology and data-hosting hub.

82 POPIA, s 72
83 Ibid, s 55
84 Information Regulator of South Africa, *Annual Performance Plan 2023/24* (2023)
85 African Union, *Convention on Cyber Security and Personal Data Protection (Malabo Convention)* (2014)
86 Ibid, arts 8–14, 25
87 AU Treaty Status Report 2024 (2024)
88 ibid

The Convention aligns with the *African Union Digital Transformation Strategy 2020–2030*, which envisions a single African digital market anchored in trust and accountability.[89] Without ratification, Kenya risks normative isolation and regulatory inconsistency, complicating data exchange within frameworks such as the *African Continental Free Trade Area (AfCFTA)*.

Incorporating Malabo obligations into domestic law would also bolster cybersecurity cooperation. Article 25 calls for coordination among national Computer Emergency Response Teams (CERTs), an area where Kenya's National KE-CERT/CC has faced resource constraints.[90] Enhanced collaboration would improve resilience against regional cyber threats that transcend national boundaries.

5.4 Summary of Comparative Lessons

From these comparative experiences, several best practices emerge that could strengthen Kenya's regulatory capacity and embed accountability into its data-governance ecosystem:

First, mandatory DPIAs and AIAs: Kenya should require data-protection and algorithmic-impact assessments for all high-risk processing, mirroring the GDPR.[91]

Second, institutional independence: Guaranteeing budgetary and operational autonomy for the ODPC would enable impartial enforcement akin to South Africa's Information Regulator.[92]

Third, algorithmic transparency: Entities should be legally obliged to document model logic, training datasets, and bias-mitigation procedures.[93]

Fourth, granular consent: Consent frameworks must be specific, revocable, and easily understandable to mitigate exploitative data practices.[94]

Fifth, regional harmonisation: Ratifying the Malabo Convention

89 African Union, *Digital Transformation Strategy 2020–2030* (2020)
90 Communications Authority of Kenya, *National Cyber Security Strategy 2022–2027* (2022)
91 GDPR, art 35
92 POPIA, s 39
93 Lilian Edwards and Michael Veale, 'Slave to the Algorithm?' [2017] 16 Duke L & Tech Rev 18
94 ODPC, *Guidance Note on Consent and Data Sharing* (2022)

would create a coherent regional privacy regime and ease cross-border enforcement.[95]

Lastly, public digital-rights education: Continuous civic education on privacy and cybersecurity would cultivate informed data subjects capable of asserting their rights.[96]

These lessons point to a paradigm of preventive regulation grounded in human dignity and democratic accountability rather than bureaucratic compliance.

6.0 Conclusion and Recommendations

Kenya's digital economy depends on data as an engine of growth and inclusion. However, without robust governance, big data risks undermining the very rights it seeks to empower. This paper has shown that Kenya's *Data Protection Act 2019* establishes a sound legal foundation but suffers from enforcement and operational weaknesses.

- A future-ready data-protection regime must be preventive, rights-based, and technologically informed. This paper recommends the following measures:
- Legislative reforms introducing explicit provisions for DPIAs and algorithmic accountability.
- Enhanced autonomy and funding for the ODPC to conduct audits and issue compliance codes.
- Adoption of proportional, risk-based compliance models akin to POPIA.
- Ratification of the Malabo Convention to foster regional cooperation.
- Public education campaigns to promote awareness of digital rights.
- Judicial and parliamentary oversight to ensure technological regulation aligns with constitutional principles.

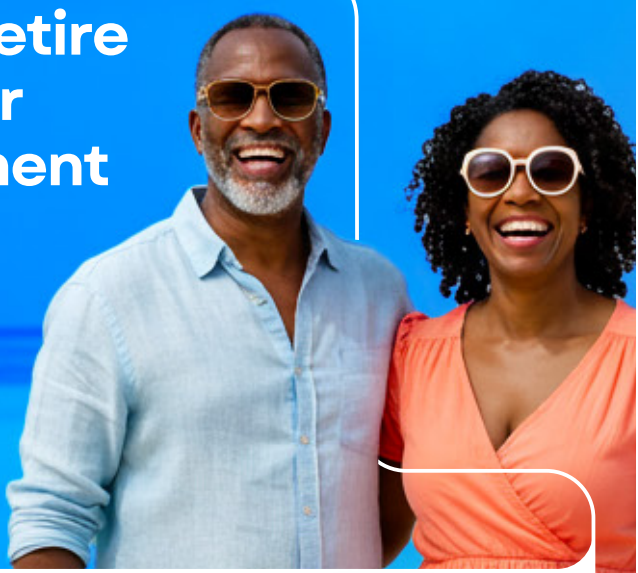
By embracing these reforms, Kenya can transform its digital landscape into one that safeguards human dignity while promoting innovation. Balancing technology and rights will ensure that the promise of big data is fulfilled without compromising the fundamental freedoms that define a democratic society.

95 African Union (Malabo Convention) (2014) arts 8–14

96 Article 19 Eastern Africa, *Public Engagement on Digital Rights 2023* (2023)

Britam | 60TH ANNIVERSARY

Live well and retire better with our Britam retirement plans



With our retirement solutions, you will enjoy these and many more benefits:

- A guaranteed minimum return of 5% per year
- Savings that are secure against market fluctuations
- Smooth and seamless expert support when transferring funds from another provider
- Affordable medical cover in retirement with Britam Afya Pension plan

Start saving now.

SMS 'PENSION' to 21778

2024 Pension Declared Net Rate

13%

*Terms and conditions apply

FRIENDS FOR LIFE

HEAD OFFICE: Britam Tower, Hospital Rd, Upper Hill
Tel: 0705100100 | **WhatsApp:** 0705100100 | **Email:** customerservice@britam.com

KENYA | UGANDA | TANZANIA | RWANDA | SOUTH SUDAN | MOZAMBIQUE | MALAWI
www.britam.com BritamEA BritamGroup

REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

Do you Collect or Process Personal Data?

Whether you're a business, NGO, government agency, school, hospital, law firm, or SACCO...if you handle names, ID numbers, contacts, or employee records, the law requires you to register as a Data Controller or Data Processor.

It's the law. It's about trust!

Register
Comply
Empower

REGISTER TODAY

www.odpc.go.ke

Disembodied Rights? Rethinking the Extension of Human Rights in the Metaverse

By Victoria W. Kariithi and Eddah M. Mwanyumba***

Abstract

The digital world is evolving at an extraordinary pace, often outpacing the capacity of the physical world to adapt in real time. At the centre of this technological evolution is Web3, the next generation of the internet, which is built on decentralised technologies, and more strikingly, the emergence of the Metaverse. This is an immersive, persistent virtual environment that increasingly mirrors and integrates with our lived experiences. Whether working, socialising, or transacting, users now extend their physical presence into digital spaces through avatars, raising novel and complex legal and ethical questions. Among these is the pressing question of whether human rights can or should be meaningfully extended to the Metaverse. The glaring truth is that technological advances and realities shape the way we live, relate, and regulate, with far-reaching consequences for society at large. This article reviews the competing perspectives on the application of human rights to the Metaverse and its digital citizens - avatars. It begins by clarifying key concepts before exploring the implications of extending rights traditionally anchored in the physical world into virtual environments. While acknowledging the need to protect human dignity and autonomy in digital spaces, the article ultimately argues against a wholesale extension of human rights into the Metaverse. Instead, it advocates for the development of alternative governance mechanisms that reflect the distinct nature of virtual interaction, while still upholding the core values that underpin human rights. The authors suggest this approach prevents premature legal overreach and rights dilution.

Keywords: *Disembodied rights, autonomy, emergent metaverse, virtual environments, evolution*

1.0 Introduction

We are living through the profound transformations of the fourth digital revolution, an era marked not only by technological innovation but by the reconfiguration of the human experience itself. This revolution is reshaping the economic, cultural, and social dimensions of life with unprecedented

velocity.[1] Among its most consequential developments is the emergence of the Metaverse, described by Cuéllar et al. as a networked, immersive environment that fundamentally alters how individuals experience presence, agency, and interaction in digital space.[2]

The Metaverse, underpinned by Extended Reality (XR) and Web3 technologies, such as Blockchain, represents far more than a novel platform for entertainment or communication. It signals a structural reimagining of how individuals' shop, work, socialise,[3] and exercise agency in digital domains. As individuals increasingly live, transact, and relate within this virtual realm, the Metaverse raises pressing normative questions about the scope, substance, and enforcement of human rights in spaces that transcend physical borders and traditional legal frameworks. The rise of the Metaverse has prompted an urgent scholarly debate about the scope and applicability of human rights in digital spaces. As individuals increasingly conduct social, professional, and economic activities through avatars, a central question emerges: can rights traditionally rooted in the corporeal world be meaningfully extended to these new, disembodied domains? Human rights, long regarded as universal entitlements inherent to all individuals, irrespective of status or geography,[4] now face both transformative potential and new threats in the digital age. The Metaverse promises enhanced access to expression, creativity, and community, potentially

1 The author wishes to acknowledge with appreciation, Allan Mwashemu for his consistent and invaluable assistance.

** Head of Commercial at Mwanyumba Kariithi & Company Advocates. Sitting member of the Advocates Disciplinary Tribunal. Bachelor of Laws (Hons), Bachelor of Arts (Sociology & Political Science) (NALSAR University of Law), Dip. in Law (Kenya School of Law), Certified Company Secretary (ICS), Associate Arbitrator (CIArb), Certified Professional Mediator (MTI) East Africa and Patent Agent.

* Managing Partner at Mwanyumba Kariithi & Company Advocates, MSc Blockchain & Digital Currency (University of Nicosia), Bachelor of Laws and Bachelor of Arts (Politics) (University of Notre Dame Australia), Dip. in Law (Kenya School of Law), Certified Blockchain & Law Professional (Blockchain Council), Certified Professional Mediator (MTI) East Africa, and a Star Trek fan.

The authors are grateful to the staff at Mwanyumba Kariithi & Company for their continued support.

Diana Peña Cuellar, Astrid Vidal Lasso and Alejandra Buriticá Salazar, 'The metaverse: an analysis from a human rights perspective' (2024) Revista Jurídica Mario Alario D'Filippo, 16(33), 202-218 <https://doi.org/10.32997/2256-2796-vol.16-num.33-2024-4889 > accessed 22nd April 2025

2 Ibid, no. 1.

3 Kuzi Charamba, 'Beyond The Corporate Responsibility To Respect Human Rights In The Dawn Of A Metaverse' (2022), 30 U. MIA Int'l & Comp. L. Rev. 110 <https://repository.law.miami.edu/umiclr/vol30/iss1/5/> accessed 22nd April 2025

4 C.C Nwufo, 'An Overview of Human Rights, Good Governance and Development' (2010) African Research Review / Vol. 4 No. 1 <https://www.ajol.info/index.php/afrrev/article/view/58220> accessed 20th April 2025

reinforcing core freedoms such as speech and assembly.[5] Yet it simultaneously introduces new vulnerabilities: biometric surveillance, algorithmic bias, data exploitation, and forms of discrimination that challenge existing regulatory paradigms.[6]

Moreover, the inherently transnational and decentralised nature of the Metaverse disrupts conventional legal definitions and assumptions that have long guided human interactions[7]. It complicates questions of jurisdiction, accountability, and sovereignty, thus demanding a reassessment of how public international law and domestic regulatory mechanisms engage with virtual environments,[8] taking a critical look at who becomes the duty bearer and who is the rights holder in this new "world". As technology evolves faster than legislation, the risk emerges that human rights protections may fall behind, ill-equipped to safeguard users in rapidly changing digital ecosystems,[9] which still expose them to the very ills that have long since been fought against and rightfully protected from.

Accordingly, this article examines whether human rights, traditionally grounded in the tangible and embodied realities of the physical world, should be extended to the Metaverse. It begins by defining key concepts - human rights, the Metaverse, Web3, and Blockchain- to ground the analysis. It then explores arguments in favour of and against extending rights into this realm. Proponents of extension argue for moral and legal continuity, citing the increasing significance of virtual identity and presence. Opponents caution against such an extension, arguing that the differences between physical and virtual experiences could cause confusion in practice, and reinforce or worsen existing inequalities.[10]

5 Katitza Rodriguez, Kurt Opsahl, Rory Mir, and Daniel Leufer, 'Virtual Worlds, Real People: Human Rights in the Metaverse' (*Electronic Frontier Foundation*, 9 December 2021) <https://www.eff.org/deeplinks/2021/12/virtual-worlds-real-people-human-rights-metaverse> accessed 22nd April 2025

6 Hatice Kübra Ecemiş Yilmaz, 'Legal Issues of the Metaverse: A Public International Law Perspective' (2024). Law and Justice Review 27, pgs. 29-68 <https://search.trdizin.gov.tr/en/yayin/detay/1258338/legal-issues-of-the-metaverse-a-public-international-law-perspective> accessed 22nd April 2025

7 Katitza Rodriguez, Kurt Opsahl, Rory Mir, and Daniel Leufer, 'Virtual Worlds, Real People: Human Rights in the Metaverse' (Electronic Frontier Foundation, 9 December 2021) <https://www.eff.org/deeplinks/2021/12/virtual-worlds-real-people-human-rights-metaverse> accessed 22nd April 2025

8 Tomer Jordi Chaffer, Justin Goldston, Gemach D.A.T.A. I, 'Incentivized Symbiosis: A Paradigm for Human-Agent Coevolution' (2024) <https://doi.org/10.48550/arXiv.2412.06855> accessed 28th April 2025

9 Shicheng Wan, Hong Lin, Wensheng Gan, Jiahui Chen, Philip S. Yu, *Web3: The Next Internet Revolution* (2023) <https://doi.org/10.48550/arXiv.2304.06111> accessed 28th April 2025

10 Sarah Cemlyn, 'Human Rights Practice: Possibilities and Pitfalls for Developing Emancipatory Social Work' (2008) Ethics and Social Welfare 2 (3): 222–42 <https://doi.org/10.1080/17496530802481714>

Ultimately, this article argues that while the aspiration to uphold dignity and autonomy in digital spaces is essential, a wholesale extension of human rights into the Metaverse is problematic. Instead, it proposes the development of alternative, context-specific procedural safeguards and digital governance frameworks. These should be tailored to the distinct conditions of virtual environments, ensuring that the Metaverse evolves as a secure and equitable space for all its users. In doing so, this article aims to contribute meaningfully to the evolving discourse on digital governance, offering a grounded, forward-looking perspective on how to ensure the Metaverse becomes a secure and equitable space for all who inhabit it. As digital life increasingly intersects with the core structures of society, this conversation is not only timely but essential.[11]

2.0 Definitions and key concepts

To meaningfully explore the implications of human rights in the rapidly evolving digital landscape of the Metaverse, it is essential to first clarify the foundational concepts that underpin this discussion, - human rights and the Metaverse, - and to briefly examine the enabling technologies that support it, namely Web3 and Blockchain. This section conceptualizes the inquiry, not by delving into technical minutiae, but by offering a grounded understanding of the evolving digital terrain in which human rights must increasingly operate. These definitions anchor our exploration of how rights, classically conceived for the physical world, might translate into and be challenged by virtual environments.

2.01 Human Rights

Human rights have, over the years, come to be universally referred to as inherent entitlements that are available to every individual globally by virtue of being a human being, regardless of race, sex, nationality, ethnicity, or religion, or any other status, and are grounded in ethical principles essential to a life of dignity.[12] They actively promote equality, dignity, and respect, and speak against discrimination. They govern the conduct of both state and non-state actors, providing a moral and legal compass for the treatment of persons across societies.[13]

accessed 28th April 2025

11 Shicheng Wan, Hong Lin, Wensheng Gan, Jiahui Chen, Philip S. Yu, 'Web3: The Next Internet Revolution' (2023) <https://doi.org/10.48550/arXiv.2304.06111> accessed 28th April 2025

12 C.C Nwufo, 'An Overview of Human Rights, Good Governance and Development' (2010) African Research Review / Vol. 4 No. 1 <https://www.ajol.info/index.php/afrrev/article/view/58220> accessed 20th April 2025

13 Stephen P. Marks, *Human Rights: A Brief Introduction. Working Paper, Harvard School of Public Health*

These rights are often described as inalienable, meaning they cannot be surrendered; interdependent, such that the fulfilment of one right enables the enjoyment of others; and indivisible, forming a coherent and inseparable whole.[14] Human rights encompass a spectrum of liberties and entitlements, including the right to life, freedom from torture, fair trial guarantees, freedom of expression, access to healthcare and education, and cultural rights tied to identity and heritage.[15]

Though the roots of human rights lie in various moral, religious, and philosophical traditions, from natural law to Kantian ethics, the contemporary international human rights system was largely institutionalised in the aftermath of the Second World War. Since then, nine core international treaties and a web of regional instruments have formalised these norms, underpinned by institutions tasked with monitoring, interpreting, and enforcing compliance.[16] Yet this framework now encounters profound challenges. As technologies like the Metaverse redefine how individuals interact, share information, and assert identity, longstanding human rights norms must be reinterpreted to meet new realities.[17] Digital privacy, data sovereignty, algorithmic bias, and equitable access are not peripheral concerns; they are now central to any modern rights discourse.[18] In this light, human rights must be understood not as static entitlements, but as adaptive principles, capable of responding to the complex demands of a digital society.[19]

2.02 The Metaverse and Avatars

There is currently no universally accepted definition of the Metaverse, though active efforts are underway to standardise and clarify its terminology.[20] However, the term's literary origin remains significant,

(2014) <https://dash.harvard.edu/entities/publication/73120378-e964-6bd4-e053-0100007fdf3b> accessed 22nd April 2025

14 Alan S. Gutterman, 'What are Human Rights?' (2023) <http://dx.doi.org/10.2139/ssrn.4320947> accessed 22nd April 2025

15 Ibid, no. 13.

16 Ibid, no. 14.

17 Liang Yang, Yan Xu and Pan Hui, 'Metaverse Identity: Core Principles and Critical Challenges' (2024) <https://www.researchgate.net/publication/381372896_Metaverse_Identity_Core_Principles_and_Critical_Challenges> accessed at 21st July 2025

18 Ibid, no. 8.

19 Neil Hibbert, 'Human Rights and Social Justice' (2017) Laws 2, 6(2), 7 <https://doi.org/10.3390/laws6020007> accessed 24th July 2025

20 Council of Europe and IEEE, 'The metaverse and its impact on human rights, the rule of law and democracy' (2024) <https://book.coe.int/en/human-rights-and-democracy/11904-the-metaverse-

as it offers an early conceptual framework for understanding the potential scope of this emerging technology.[21] Originally coined by Neal Stephenson in his 1992 novel Snow Crash, the "Metaverse" described a cyberpunk world where users, represented by avatars, engaged with one another in a shared virtual environment.[22] Scholars such as Qin, *et al.*, Cuellar *et al.,* Yilmaz, Caballero and Balbuena have since referenced this origin in defining the concept.[23] Though fictional in origin, the Metaverse has evolved into a tangible and increasingly complex digital ecosystem. According to Qin *et al.*, the Metaverse is widely regarded as "a yet-to-be realized augmentation of the Internet".[24] A boundaryless space where physical reality converges with multiple virtual worlds, transcending time and geographic limitations.[25] It is also referred to as an immersive, three-dimensional virtual space where users can engage in lifelike personal and professional interactions, supported by Extended Reality technologies such as virtual reality (VR), augmented reality (AR), and mixed reality (MR)[26] and diminished reality (DR).[27]

---

and-its-impact-on-human-rights-the-rule-of-law-and-democracy.html> accessed 20th April 2025

21 Joxerramon Bengoetxea Caballero and Roberto Leopoldo Cruz Balbuena, 'Institutions of law in the metaverse' (2024) Oñati Socio-Legal Series Volume 14, Issue 6(2024),1531–1554 <https://opo.iisj.net/index.php/osls/article/view/1852/2365> accessed 20th April 2025

22 Ibid, no. 6.

23 Ibid no. 1.

24 Hua Xuan Qin, Yuyang Wang and Pan Hui, 'Identity, crimes, and law enforcement in the Metaverse' (2025). Humanit Soc Sci Commun 12, 194 (2025) <https://doi.org/10.1057/s41599-024-04266-w> accessed 20th April 2025

25 Ibid, no. 1.

26 Ibid, no. 6.

cf Ayşe Meriç Yazıcı, Ayşegül Özkan & Hasan Özkan, 'Meta: XR-AR-MR and Mirror World Technologies Business Impact of Metaverse*'* (2024) Volume: 4 Issue: 1, 21 – 32 Journal of Metaverse <https://dergipark.org.tr/en/pub/jmv/issue/76655/1344489> accessed 20th April 2025

Virtual Reality (VR) is an immersive and interactive simulated environment that is experienced in the first person and provides a strong sense of presence to the user. Augmented Reality (AR) is an immersive and interactive environment in which virtual content is spatially registered to the real world and experienced in the first person, providing a strong sense of presence in a combined real / virtual space - see Louis Rosenberg. (2022). Regulation of the Metaverse: A Roadmap: The risks and regulatory solutions for largescale consumer platforms. See Diana Peña Cuellar, Astrid Vidal Lasso and Alejandra Buriticá Salazar, 'The metaverse: an analysis from a human rights perspective' (2024) Revista Jurídica Mario Alario D'Filippo, 16(33), 202-218 <https://doi.org/10.32997/2256-2796-vol.16-num.33-2024-4889 > accessed 22nd April 2025

Mixed reality (MR): Combines elements from both VR and AR, for example by using VR headsets to work in a virtual meeting room or office, where you can use several virtual screens, and also see the physical screen and keyboard. Diminished reality (DR): A data-generated environment where you can reduce and remove physical surroundings and replace them with virtual elements. – see Tore Tennøe and Adele Matheson Mestad 'The Metaverse and Human Rights' (*Norwegian Human Rights Institution*, 5 December 2022) <https://www.nhri.no/en/report/the-metaverse-and-human-rights/?showall=true> accessed 20th April 2025

27 Tore Tennøe and Adele Matheson Mestad 'The Metaverse and Human Rights' (*Norwegian Human*

Artificial intelligence (AI) is also central in shaping the Metaverse experience, serving as both an engine of personalization and a tool for dynamic interaction. It analyses users' preferences, behaviours, and patterns in real time, enabling adaptive environments that respond intelligently to individual needs. This enhances both the efficiency and personal relevance of virtual interactions within the Metaverse.[28] It enables more lifelike avatars, now capable of simulating full-body movement, to infer motion from limited data inputs.[29] In addition, AI supports real-time translation, content creation, and environment rendering, making it a vital engine behind the interactive and human-centred nature of the Metaverse.[30]

Etymologically, "metaverse" fuses the Greek "meta" (beyond) with "universe," implying a domain that transcends the physical and exists in virtual form. In practice, the Metaverse represents a digital infrastructure that facilitates real-time interaction, social engagement, and economic exchange. At the heart of this experience are avatars, customisable digital representations of users, which function as embodied proxies through which individuals navigate virtual spaces. These avatars allow users to interact with digital objects, participate in virtual economies (such as trading goods, services, or real estate), and engage in a broad range of activities, including education, work, entertainment, and social life.[31]

2.03 Web3 and Blockchain

Web3 represents the next evolution of the internet, moving from static webpages (Web1), through interactive social platforms (Web2), to a decentralised, user-centric digital architecture. Web3 combines technologies like Blockchain, smart contracts, cryptocurrencies[32]

Rights Institution, 5 December 2022) <https://www.nhri.no/en/report/the-metaverse-and-human-rights/?showall=true> accessed 20th April 2025

cf Louis Rosenberg, 'Regulation of the Metaverse: A Roadmap: The risks and regulatory solutions for largescale consumer platforms' (2022) ACM Digital Library <https://doi.org/10.1145/3546607.3546611> accessed 28th April 2025

28 Ibid no. 1.

29 Ibid no. 27.

30 Ibid, no. 1.

31 Stelios Ioannıdıs and Alexios Patapios Kontıs, 'The 4 Epochs of the Metaverse' (2023) Volume: 3 Issue: 2, 152 – 165 Journal of Metaverse <https://doi.org/10.57019/jmv.1294970> accessed 28th April 2025

32 "Smart contracts" is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform – see Stuart D. Levi & Alex B. Lipton, 'An Introduction to Smart Contracts and Their Potential and Inherent Limitations' (*Harvard Law*

and the Metaverse to offer a more autonomous and resilient web experience.[33] Web1 (the early web) was largely passive, allowing users only to read content.[34] Web2 introduced interactivity, enabling content creation, social networking, and user participation, but also centralised data control under major platforms.[35] Web3 now seeks to decentralise this control, returning ownership of data and digital identity to users themselves through cryptographic technologies and decentralised governance.[36]

In this context, Blockchain is not merely an enabling tool but the backbone of Web3's decentralised ethos, ensuring transparency, accountability, and resilience. Blockchain, which ensures tamper-proof data integrity and enables user sovereignty, has emerged as a foundational pillar of the new digital order.[37] It underpins much of the infrastructure that supports both Web3 and the Metaverse. At its core, Blockchain is a decentralised digital ledger that records transactions across a distributed network of computers,[38] and unlike centralised systems, it removes single points of control, enhancing transparency and security.[39] It is defined by four core attributes: immutability, decentralisation, consensus, and transparency.[40] Its role in the Metaverse is particularly significant: Blockchain enables secure,

School Forum on Corporate Governance, 26 May 2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 30th July 2025

33 Gavin Wood, 'Why We Need Web 3.0.' (*Medium*, 12 September 2018) <https://gavofyork.medium.com/why-we-need-web-3-0-5da4f2bf95ab> accessed 28th April 2025
cf Qin Wang, Rujia Li, Qi Wang, Shiping Chen, Mark Ryan, Thomas Hardjono, 'Exploring Web3 from the View of Blockchain' (2022) <https://doi.org/10.48550/arXiv.2206.08821> accessed 28th April 2025

34 Ragnedda, M., & Destefanis, G, 'Blockchain: A disruptive technology' in Ragnedda M. & Destefanis, G. (Eds.), *Blockchain and Web 3.0: Social, economic, and technological challenges* (2019) (pp. 1-11) Routledge, Taylor & Francis Group.

35 Collin Connors & Dilip Sarkar, *'Benefits and Limitations of Web3'* (2024) <https://arxiv.org/html/2402.04897v1> accessed 28th April 2025

36 Ibid no.1.

37 Victoria Kariithi, 'Navigating the Web3 Revolution: Regulatory Strategies for Kenya' (2024) Vol. 4 No. 1 Journal of Intellectual Property and Information Technology (JIPIT) <https://doi.org/10.52907/jipit.v4i1.504> accessed 28th April 2025

38 Iyolita Islam, Kazi Md. Munim, Shahrima Jannat Oishwee, A.K.M. Najmul Islam and Muhammad Nazrul Islam, 'A Critical Review of Concepts, Benefits, and Pitfalls of Blockchain Technology Using Concept Map' (2020) <https://doi.org/10.48550/arXiv.2004.08671> accessed 28th April 2025

39 Ibid no. 37.

40 Karim Sultan, Umar Ruhi & Rubina Lakhani, 'Conceptualizing Blockchains: Characteristics & Applications' (2018) <https://www.researchgate.net/publication/325464908_Conceptualizing_Blockchains_Characteristics_Applications> accessed 28th April 2025

verifiable digital ownership through Non-Fungible Tokens (NFTs)[41], supports smart contract deployment and decentralised economies, and offers a structure of trust in environments otherwise lacking conventional regulation.

2.04 Intersection of Human Rights and the Metaverse

Essentially, the Metaverse represents a new digital frontier, an immersive, three-dimensional environment that transcends the limitations of the physical world.[42] Supported by foundational technologies discussed above, such as Blockchain, artificial intelligence (AI), and extended reality (XR), the Metaverse is not merely a technological novelty but a transformative socio-digital space.[43]

As this virtual ecosystem continues to evolve, it redefines how humans interact, learn, work, and even express identity and autonomy. However, this evolution also introduces complex new challenges, particularly in the domain of human rights. The rapid convergence of our digital and physical lives necessitates critical reflection: *how do the rights we have historically protected in the physical world apply within these immersive, borderless environments?* The Electronic Frontier Foundation states that the Metaverse holds the potential to enhance certain rights, offering innovative spaces for freedom of expression, education, assembly, and political participation.[44] At the same time, it also introduces risks: heightened surveillance, unchecked data extraction, algorithmic bias, and new modalities of exclusion, harassment, and violence, many of which current legal frameworks are ill-equipped to address.[45][46]

41 A non-fungible token (NFT) is a type of cryptographic token that represents a unique asset. NFTs are tokenized versions of digital or real-world assets. They function as verifiable proofs of authenticity and ownership within a blockchain network. NFTs are not interchangeable with each other and introduce scarcity to the digital world – see John Ma, 'Non-Fungible Token (NFT)' (*Binance Academy*, 2025) <https://academy.binance.com/en/glossary/non-fungible-token-nft> accessed 30th July 2025

42 McKinsey & Company, 'What is the metaverse?' (McKinsey & Company, 17 August 2022) <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse> accessed 28th April 2025

43 Ibid no. 6.
cf Ayşe Meriç Yazıcı, Ayşegül Özkan & Hasan Özkan, 'Meta: XR-AR-MR and Mirror World Technologies Business Impact of Metaverse' (2024) Volume: 4 Issue: 1, 21 – 32 Journal of Metaverse <https://dergipark.org.tr/en/pub/jmv/issue/76655/1344489> accessed 20th April 2025
McKinsey & Company, 'What is the metaverse?' (McKinsey & Company, 17 August 2022) <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse> accessed 28th April 2025

44 Ibid no. 7.

45 Ibid, no. 6.

46 Ibid, no. 8.

Accordingly, a pressing question emerges: *do we adapt existing human rights norms to this new virtual context, or do we need an entirely new paradigm, perhaps a distinct body of "digital human rights"?*[47] This concern is not merely notional. The Norwegian Human Rights Institute observes that within the Metaverse, a user may appear on a virtual Parisian boulevard while seated in a suburban apartment in Oslo. But if a violation occurs, be it biometric surveillance or targeted discrimination, who is responsible? Is it the user's home state, the platform provider, the VR hardware manufacturer, or the creator of the digital environment?[48]

Some suggest that the Metaverse will remain a parallel digital universe, separate from the physical world in which our rights were originally conceived. Others envision a fully integrated extended reality, wherein virtual elements become enmeshed with our tangible lives, fundamentally altering the space in which rights are exercised and protected.[49] This tension brings us to a central philosophical and legal challenge: *can human rights, grounded in the corporeal and moral dimensions of personhood, be meaningfully transferred and applied into a disembodied virtual space? Or does the Metaverse require a re-articulation of rights that acknowledges its unique affordances and risks?*

As we shall explore in the following sections, the interplay between the physical and virtual worlds is neither binary nor static. Instead, it is fluid, dynamic, and reciprocal, raising difficult but necessary questions about how dignity, justice, and accountability can be safeguarded across both realities. The Metaverse invites us not only to reimagine digital space, but also to reconsider how, and for whom, human rights are secured in the digital age. From the foregoing discourse, it becomes apparent that it is necessary to have a structured foundation for understanding the digital terrain in which human rights may be reimagined and we dare say enforced. This re-imagination is not without limitations and implicit assumptions that warrant critical reflection.

To begin with, the idea that both concepts, human rights and the Metaverse, are relatively stable and internally coherent may be disputed, when in practice both are deeply contested, ever evolving,

47 Ibid, no. 27.
48 Ibid, no. 8.
49 Ibid, no. 27.

and shaped by political, cultural, and technological contingencies. Human rights, though presented as universal, remain subject to divergent interpretations across jurisdictions and traditions, an issue that becomes more acute in the transnational and pluralistic context of the Metaverse. Moreover, the framing of this proposition assumes that human rights can simply be adapted or extended into virtual environments. While useful, it overlooks a deeper shift: the Metaverse may not just replicate physical world interactions but create entirely new forms of identity, agency, and harm that conventional legal categories and jurisprudence cannot address.

Further, the definition of the Metaverse leans toward a technologically deterministic view, suggesting that the form and implications of the Metaverse are driven chiefly by innovation. This underplays the normative and regulatory choices that will ultimately shape its development. Whether the Metaverse evolves as a site of freedom, exclusion, or surveillance will depend as much on law, governance, and collective values as on code and architecture. These limitations do not detract from the value of the conceptual groundwork laid here but rather highlight the need for ongoing critical scrutiny as we move from definitional clarity toward normative evaluation.

3.0 Extending Human Rights into the Metaverse

Although the Metaverse has attracted significant academic, political, and social attention, relatively few studies have seriously engaged with the question of how, or whether, human rights should extend into this emerging domain. Invariably, the discourse divides scholars into two broad camps: those who advocate for the adaptation of existing human rights frameworks to govern digital environments, and those who caution against such an extension. To provide a balanced foundation for the final proposition of this article, both perspectives will be critically examined. At the heart of this debate lies a deceptively simple yet far-reaching question*: if human rights are grounded in our shared dignity, equality, and freedom, why should they not follow us into the Metaverse?*[50] A growing body of scholarship responds affirmatively, contending that these rights must be reinterpreted to account for the realities of our digital selves, our avatars, and immersive interactions. The Metaverse – this new frontier challenges the adequacy of existing legal frameworks, particularly in relation to the scope and applicability of human rights.

50 Ibid, no. 8.

As it becomes more integrated into the social, economic, and political fabric of daily life, the Metaverse poses deep challenges to the adequacy of current legal norms, especially those designed to protect fundamental rights. Long-standing human rights principles, traditionally rooted in the physical world, are being tested in environments that complicate familiar notions of presence, identity, and responsibility. This shift necessitates a re-examination of what it means to protect human dignity, privacy, and autonomy in spaces that are immersive, interactive, and often unbounded by national jurisdiction. Drawing on the insights of scholars such as Cheong, Kostenko, Raposo, and Chawki, this section considers the extent to which human rights principles ought to be applied within the Metaverse. While the proposition remains contested, the argument advanced here is that extending core human rights into virtual spaces is not merely desirable but necessary to safeguard against emerging forms of injustice and to uphold the dignity and autonomy of individuals who increasingly inhabit these digital realms.

3.01 The Metaverse as a New Frontier for Human Rights

Building on the preceding overview, the evolution of avatars from passive digital proxies to autonomous, interactive agents reflects the Metaverse's emergence as a complex socio-technical ecosystem.[51] This transformation elevates virtual experiences beyond mere simulation, establishing environments where human users invest identity, emotion, and agency. As avatars increasingly serve as extensions of self, the harms they encounter cannot be dismissed as inconsequential or purely symbolic.

Accounts of virtual groping and simulated sexual assault underscore the real psychological and emotional toll such violations can inflict, particularly within immersive settings where users experience interactions with a heightened sense of presence.[52] These incidents mirror violations already codified in physical-world legal systems, yet they occur in spaces that remain largely unregulated.[53] As such, the absence of adequate legal oversight in the Metaverse creates opportunities for exploitation and abuse, particularly for vulnerable

51 Ben Chester Cheong, 'The Rise of AI Avatars: Legal Personhood, Rights and Liabilities in an Evolving Metaverse' (2024) Vol 2, No. 4 Journal of Digital Technologies and Law <https://doi.org/10.21202/jdtl.2024.42> accessed 22nd April 2025

52 Mohamed Chawki, Subhajit Basu and Kyung-Shick Choi, 'Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety' (2024) Laws 13, no. 3: 33 <https://doi.org/10.3390/laws13030033> accessed 22nd April 2025

53 Ibid, no. 51.

users.[54] For example, there are alarming patterns of predatory behaviour targeting children in virtual environments, raising urgent concerns about safeguarding and accountability.[55]

In response to these dangers, scholars such as Cheong and Kostenko *et al*. argue for the establishment of comprehensive Metaverse Codes, digital constitutional frameworks capable of governing user behaviour, platform responsibilities, and the resolution of disputes.[56] These codes, they contend, must incorporate core human rights principles to prevent the emergence of a fragmented, inequitable digital society. The risk, as they highlight, is that without these protections, the Metaverse will not only reproduce but also amplify existing social inequalities and asymmetries of power.[57]

Moreover, the immersive nature of virtual environments blurs the lines between online and offline experiences. When harm occurs in such settings, the psychological impact is no less significant simply because the event took place in a virtual domain.[58] This collapse of the boundary between physical and digital presence complicates any rigid separation between real-world law and virtual conduct. It also supports the proposition that fundamental protections such as the rights to privacy, dignity, and freedom from discrimination must find meaningful expression in the Metaverse.[59]

However, while the imperative to protect users from harm is clear, the way these rights are applied in virtual settings remains contested. As this article argues, simply transposing the existing human rights

54 RR Krishnaa, 'Challenges in the Metaverse Jurisdiction and International Treaty Law' (2023) Vol 2023 Intergovernmental Research and Policy Journal <https://irpj.euclid.int/articles/challenges-in-the-metaverse-jurisdiction-and-international-treaty-law/ > accessed 22nd April 2025

55 Catherine Allen and Verity McIntosh, 'Child Safeguarding and Immersive Technologies an Outline of the Risks' (*NSPCC*, 2023) <https://www.careknowledge.com/media/56792/child-safeguarding-immersive-technologies.pdf> accessed 30th July 2025

56 Ibid no. 51.

57 Ibid, no. 57.

58 Yogesh K. Dwivedi, Laurie Hughes, Abdullah M. Baabdullah, Samuel Ribeiro-Navarrete, Mihalis Giannakis, Mutaz M. Al-Debei, Denis Dennehy, Bhimaraya Metri, Dimitrios Buhalis, Christy M.K. Cheung, Kieran Conboy, Ronan Doyle, Rameshwar Dubey, Vincent Dutot, Reto Felix, D.P. Goyal, Anders Gustafsson, Chris Hinsch, Ikram Jebabli, Marijn Janssen & Samuel Fosso Wamba, 'Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy' (2022) Volume 66 International Journal of Information Management <https://www.sciencedirect.com/science/article/pii/S0268401222000767 > accessed 28th July 2025

59 Council of Europe and IEEE, 'The metaverse and its impact on human rights, the rule of law and democracy' (2024).

framework into a digital context risks conceptual distortion and practical ineffectiveness. Still, the case for a structured and principled response to virtual harms remains strong. Without it, the Metaverse risks becoming a space in which human dignity is compromised under the guise of innovation.

3.02 Avatars as Legal Persons

A more contested proposition within the growing discourse on legal personhood in the Metaverse involves the recognition of avatars as legal persons endowed with rights and responsibilities. It has been suggested that AI-driven avatars could, under the principles laid out in the English case of *Salomon v Salomon,*[60] be granted a legal status analogous to that of corporations in common law.[61] The *Salomon* principles provide that a company is essentially regarded as a legal person separate from its directors, shareholders, employees and agents. This means as a separate legal entity, a company can be sued in its own name and own assets separately from its shareholders. The corporate veil is drawn from the *Salomon* principle which separates the rights and duties of the company from the rights and duties of the shareholders and directors. Essentially, the corporate veil is a metaphoric veil with the company on one side of it and its directors and shareholders on the other and liability does not pass through. The corporate veil does not provide protection to its shareholders and directors for their personal conduct or allow companies to be used for sham transactions. Accordingly, the courts may lift or pierce the corporate veil. In this model, avatars would not merely act as user-controlled representations but could be incorporated as distinct legal entities with the capacity to own property, enter contracts, and incur liabilities.

This claim finds further support in the work of Raposo, who notes that AI-powered avatars are already performing autonomous tasks, including negotiating agreements and producing copyrighted content.[62] The justification for extending legal status to such entities stems not from their sentience, since they possess none, but from their

60 *Salomon v Salomon* [1897] AC 22.

61 Ibid no. 51.

62 Vera Lucia Raposo, 'Beyond Pixels and Profiles: Unveiling the Legal Identity of Avatars in the Metaverse' (2024) *Proceedings of the International Congress Towards a Responsible Development of the Metaverse*, Alicante, 13-14 <https://catedrametaverso.ua.es/wp-content/uploads/2024/07/Beyond-Pixels-and-Profiles-Unveiling-the-Legal-Identity-of-Avatars-in-the-Metaverse-RAPOSO.pdf > accessed 22nd April 2025

demonstrable autonomy and growing participation in economically and creatively significant activities, such as making decisions and even influencing behaviours.[63] Like corporations, which are afforded legal personhood despite their lack of consciousness, avatars arguably merit similar treatment based on their functional capabilities.[64]

As Mengual emphasises, the threshold for legal personhood is not humanity, but autonomy: the ability to act independently and produce real-world outcomes.[65] Recognising this would allow avatars to be held directly accountable for virtual offences, such as digital theft or contractual breaches, and would mitigate the jurisdictional and evidentiary complexities associated with tracing such acts to human users across dispersed networks and legal systems.[66] Accordingly, personified avatars also provide a clear locus for responsibility. Holding an avatar itself to account for harassment or property damage avoids the impracticality of tracing actions through anonymous networks or multiple jurisdictions.[67] However, effective enforcement would require avatars to be vested with procedural guarantees, for example, the right to a fair trial, that reflect core human rights protections. In effect, establishing avatar personhood would compel the translation of principles such as due process, equality before the law, or protection from arbitrary detention into the Metaverse's legal architecture.[68]

Nonetheless, the argument that avatars merit some form of legal protection is not without emotional and ethical resonance. Cheong emphasises that avatars are more than strings of code; they are increasingly integral to our identities.[69] Attacks on avatars, whether

63 Ibid no. 51.

64 Ibid no. 51.

cf Lorena Arismendy Mengual, 'A legal status for Avatars in the Metaverse from a Private Law perspective' (InDret, 9 April 2024) <https://indret.com/wp-content/uploads/2024/04/1862.pdf > accessed 22nd April 2025

65 Lorena Arismendy Mengual, 'A legal status for Avatars in the Metaverse from a Private Law perspective' (InDret, 9 April 2024) <https://indret.com/wp-content/uploads/2024/04/1862.pdf > accessed 22nd April 2025

66 Ibid, no. 65.

67 Hua Xuan Qin, Yuyang Wang and Pan Hui, 'Identity, crimes, and law enforcement in the Metaverse' (2025). Humanit Soc Sci Commun 12, 194 <https://doi.org/10.1057/s41599-024-04266-w> accessed 20th April 2025

cf Zachary Schaengold, 'Personal Jurisdiction Over Offenses Committed in Virtual Worlds' (2013) University of Cincinnati Law Review, Vol. 81, Iss. 1, Art. 10 <https://scholarship.law.uc.edu/cgi/viewcontent.cgi?article=1098&context=uclr > accessed 29th July 2025

68 Ibid, no. 51.

69 Ibid, no. 51.

through theft, manipulation, or humiliation, can produce real psychological distress. Without a legal framework to recognise and redress such injuries, the Metaverse risks becoming an unequal and unsafe space, particularly for marginalised users.[70] This moral claim demands a jurisprudence that takes seriously the entanglement of virtual and real harms.

3.03 Safeguarding Vulnerable Populations in the Metaverse

It is crucial to recognize the human dimension of the Metaverse, as it is a space where individuals, including children and adolescents, engage in activities such as gaming and identity formation. Chawki and Krishnaa draw attention to the significant risks present within the Metaverse, including sexual exploitation, bullying, and discrimination, which disproportionately affect vulnerable populations.[71] Incidents such as the groping of female avatars, occurrences reported by the BBC.[72] The fraudulent deprivation of a young user's virtual assets has profound emotional and economic consequences.[73] Furthermore, Tu & de Castro e Silva highlight the potential for data misuse and surveillance within the Metaverse, which poses additional threats to privacy and equality.[74] In this context, the application of human rights principles, such as the right to freedom from sexual harassment, right to privacy, right to health, dignity, right to equality, and freedom from discrimination, is not merely desirable but essential to ensure that the Metaverse serves as a space for positive development rather than harm.

---

70 Ibid, no. 51.

cf Lorena Arismendy Mengual, 'A legal status for Avatars in the Metaverse from a Private Law perspective' (InDret, 9 April 2024) <https://indret.com/wp-content/uploads/2024/04/1862.pdf > accessed 22nd April 2025

71 Mohamed Chawki, Subhajit Basu and Kyung-Shick Choi, 'Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety' (2024) Laws 13, no. 3: 33 <https://doi.org/10.3390/laws13030033> accessed 22nd April 2025

cf RR Krishnaa, 'Challenges in the Metaverse Jurisdiction and International Treaty Law' (2023) Vol 2023 Intergovernmental Research And Policy Journal <https://irpj.euclid.int/articles/challenges-in-the-metaverse-jurisdiction-and-international-treaty-law/ > accessed 22nd April 2025

72 BBC, 'Female avatar sexually assaulted in Meta VR platform, campaigners say' *BBC* (25 May 2022) <https://www.bbc.com/news/technology-61573661 > accessed 24th July 2025

cf Chris Vallance 'Police investigate virtual sex assault on girl's avatar' *BBC* (3 January 2024) <https://www.bbc.com/news/technology-67865327 > accessed 24th Julu 2025

73 Rebecca Cole, 'A qualitative investigation of the emotional, physiological, financial, and legal consequences of online romance scams in the United States' (2024) Volume 6 Journal of Economic Criminology <https://doi.org/10.1016/j.jeconc.2024.100108> accessed at 24th July 2025

74 Xinyi Tu and Bruna de Castro e Silva, 'Are We Ready for the Metaverse? Implications, Legal Landscape, and Recommendations for Responsible Development' (2025) Digit. Soc. 4, 9 <https://doi.org/10.1007/s44206-025-00163-0> accessed 22nd April 2025

As the Metaverse continues to evolve, it appears that it is not merely a space of digital novelty. It is one where individuals, including children, adolescents, and other at-risk groups, participate in gaming, social interaction, economic exchange, and, significantly, identity formation. This human presence renders the Metaverse not just a technological construct, but a social environment fraught with ethical and legal implications.[75] Chawki underscores the serious risks facing vulnerable users in these spaces, including sexual exploitation, bullying, discriminatory conduct, and manipulation. These harms are not hypothetical, as revealed in the paragraph above.[76] These digital experiences may be mediated through screens or headsets, but their emotional and social impact is real and, in many cases, severe. Tu and de Castro e Silva further highlight the pervasive risk of surveillance and data misuse in the Metaverse, drawing attention to how virtual platforms harvest user data with minimal oversight, often undermining the rights to privacy, equality, and autonomy. When these intrusions disproportionately affect children, the elderly, and marginalised groups, they deepen existing structural vulnerabilities and reinforce digital inequality.[77]

Further, one of the most urgent concerns lies in the concept of digital dignity. Charamba's work offers a compelling examination of how avatars, despite being code-based entities, are deeply intertwined with users' identities and thus susceptible to identity-based harm. Forms of abuse such as hate speech, "virtual groping," and deepfake manipulation can inflict psychological distress on users, particularly when those avatars are extensions of one's self-concept.[78] The experience reported by a beta tester on Meta's Horizon Worlds, who faced a virtual assault, illustrates the emotional gravity of such interactions; even the platform acknowledged the harm.[79] If "virtual reality is genuine reality," then

75 Ibid no. 51.

cf Margarita Robles-Carrillo, 'Digital identity: an approach to its nature, concept, and functionalities' (2024) International Journal of Law and Information Technology, Volume 32, eaae019 <https://doi.org/10.1093/ijlit/eaae019 > accessed 29th July 2025

76 Ibid no. 71.

77 Ibid no. 74.

78 Kuzi Charamba, 'Beyond The Corporate Responsibility to Respect Human Rights in the Dawn of a Metaverse' (2022) 30 U. MIA Int'l & Comp. L. Rev. 110 <https://repository.law.miami.edu/umiclr/vol30/iss1/5/ > accessed 22nd April 2025

79 Tanya Basu, 'The metaverse has a groping problem already' (MIT Technology Review, 16 December 2021) <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/> accessed 29th July 2025

the legal obligations imposed on digital platforms must mirror those expected of states in the physical world.[80] This would entail incorporating anti-discrimination mandates from instruments such as the Constitution of Kenya, directly into the governance structures of virtual platforms, through platform codes of conduct, algorithmic accountability, and liability provisions for operators who fail to prevent or adequately respond to harm.

Equally pressing is the need for structural safeguards tailored to the most vulnerable. Studies by Charamba and others reveal how immersive technologies, especially those employing haptic feedback and hyper-realistic graphics, magnify the risks of sexual exploitation, cyberbullying, and covert surveillance, particularly for children, the elderly, and those with cognitive vulnerabilities. These harms are not only intensified by the sensory realism of extended reality (XR) but also by the lack of age-appropriate protective mechanisms and regulatory clarity.[81]

In this setting, the integration of human rights principles, such as the right to freedom from sexual harassment, the right to privacy, the right to health and dignity, and the freedom from discrimination, is not merely an inclination. It is a moral and legal imperative. Without such protections, the Metaverse risks replicating and amplifying the very injustices human rights were designed to prevent.[82] A meaningful human rights framework for the Metaverse must therefore extend beyond abstract declarations. It must integrate enforceable child-protection norms drawn from instruments such as the United Nations Convention on the Rights of the Child (UNCRC), ensure that consent in immersive spaces is informed and continuous, not simply the acceptance of lengthy click-wrap agreements, and explore emergent protections such as "neurorights"[83] that safeguard users' mental privacy and cognitive freedom against subliminal influence and neuro-invasive technologies.

80 Ibid, no. 74.

81 Ibid, no. 79.

82 Ibid, no. 78.

83 Neurorights could be defined as ethical, legal, social or natural principles of freedom or entitlement related to a person's cerebral and mental domain - European Parliament, 'Neurotechnology and neurorights - Privacy's last frontier' (*Think Tank, European Parliament,* 16 November 2023) <https://www.europarl.europa.eu/thinktank/de/events/details/neurotechnology-and-neurorights-privacy-/20231019WKS05721 > accessed 29th July 2025

3.04 Economic and Property Rights in the Metaverse

Economic activity in the Metaverse has outgrown the realm of pure recreation, evolving into complex virtual economies where digital assets, from land and avatars to Non-Fungible Tokens (NFTs) and cryptocurrencies, carry substantial real-world value.[84] Wealth generated in these spaces can also be expropriated: theft or sabotage of digital holdings inflicts losses that mirror their physical world equivalents, a point Qin *et al*. underscore in arguing for the legal recognition of virtual property.[85] They argue that to treat virtual assets as legally inconsequential is a fiction that undercuts users' economic security and paves the way for predatory practices and platform instability.

Virtual property crimes are far from hypothetical. Users routinely report vandalism of digital art, such as graffiti in shared virtual galleries, that becomes irremediable when original data are overwritten without backup.[86] Scams and hacks can strip players of avatar accessories, platform-specific currencies like Robux,[87] or Blockchain-based tokens.[88] Because many platforms allow conversion between digital and fiat currencies, such losses translate directly into real-world financial harm.[89] Yet end-user licence agreements too often reserve broad rights for platform operators, leaving individual users legally vulnerable to dispossession by fine print rather than force.[90]

A growing judicial consensus in jurisdictions including Japan, the Netherlands, and the United Kingdom holds that deprivation of a virtual "thing" merits legal redress when it demonstrably bears "real" monetary value, i.e. is bought or sold for fiat currency.[91] However, disagreement persists over what qualifies as "real" value, leading courts in some cases to dismiss claims over smaller virtual items.[92] This

84 Ibid no. 67.
85 Ibid, no. 83.
86 Ibid no. 67.
S. Sivaranjini, Digital Vandalism and Artistic Expression: Navigating the Intersection of Media, Art, and Ethics. (2025) 6. 1 <https://www.researchgate.net/publication/388754336_Digital_Vandalism_and_Artistic_Expression_Navigating_the_Intersection_of_Media_Art_and_Ethics > accessed 29th July 2025
87 Olivia Carville and Cecilia D'Anastasio, 'Roblox's Pedophile Problem' (*Bloomberg,* 22 July 2024) <https://www.bloomberg.com/features/2024-roblox-pedophile-problem/ > accessed 29th July 2025
88 Ibid no. 67.
89 Ibid, no. 87.
90 Ibid, no. 67.
91 Ibid, no. 87.
92 Ibid, no. 67.

patchwork approach leaves significant gaps, particularly affecting users of modest means whose digital property may escape protection simply because its value is disputed.

Accordingly, international human rights law has long recognised property as a fundamental right. Article 40 of the Constitution of Kenya[93] and Article 17 of the Universal Declaration of Human Rights[94] affirms everyone's right to own property and to be protected from arbitrary deprivation, while Article 1 of Protocol No. 1 to the European Convention on Human Rights guarantees the peaceful enjoyment of possessions.[95] Extending these protections into the Metaverse is a logical and principled step: virtual assets underpin users' livelihoods, self-expression, and social participation, and so warrant the same legal safeguards as physical-world property.[96] A human rights–based approach would require states and platforms to ensure clear definitions of digital ownership, effective dispute resolution processes, and enforceable remedies for expropriation. Embedding property rights within a human-rights framework upholds the rule of law in this digital frontier, prevents a new form of "digital serfdom," and builds confidence and investment in the Metaverse without stifling its innovative potential.[97]

Ultimately, the extension of human rights into the Metaverse is neither an abstract indulgence nor an inevitable conclusion. The Metaverse does indeed represent a significant milestone in the evolution of digital technology, offering unprecedented opportunities for connection, creativity, and commerce. The arguments in favour are compelling: AI avatars are transforming our digital presence, legal voids expose users to harm, and virtual economies are now entangled with real-world value systems. Yet the challenges are profound. The absence of

93 Constitution of Kenya, 2010, Art. 40

94 Universal Declaration of Human Rights. 1948, Art. 17

95 Equality and Human Rights Commission 'Article 1 of the First Protocol: Protection of property' (*Equality and Human Rights Commission*, 4 May 2016) <https://www.equalityhumanrights.com/human-rights/human-rights-act/article-1-first-protocol-protection-property > accessed 29th July 2025

96 Craig Kevin and Iseoluwa John, 'Regulating the Metaverse: Emerging Legal Challenges in Virtual Worlds' (2025) <https://www.researchgate.net/publication/387970777_Regulating_the_Metaverse_Emerging_Legal_Challenges_in_Virtual_Worlds > accessed 29th July 2025

97 Dominic Chalmers, Suwen Chen, Yanto Chandra and Felix Honecker, 'Non-Fungible Token Innovation' Oxford Research Encyclopedia of Business and Management (*Oxford University Press*, 20 May 2025) <https://oxfordre.com/business/view/10.1093/acrefore/9780190224851.001.0001/acrefore-9780190224851-e-432 > accessed 29th July 2025

consciousness, the fragility of enforcement mechanisms, and the risk of overregulation all caution against uncritical transplantation of real-world legal frameworks. Perhaps the path forward must be carefully calibrated and bespoke. The Metaverse is not merely a technological novelty; it is an emerging *locus* of human interaction and identity. Its governance will shape the moral and legal contours of the digital age.

4.0 Why the Metaverse Cannot Sustain a Human Rights Framework

While some scholars argue for the extension of human rights into the Metaverse, as seen in the previous section, others raise serious concerns about whether this is appropriate or even possible. They point out that the Metaverse is still in its early stages; an evolving, fragmented space with no clear structure, rules, or shared understanding. Unlike the physical world, it lacks defined borders, state authorities, or stable institutions, making it difficult to apply legal principles designed for real-world societies. This section presents key arguments from scholars who caution that applying human rights to the Metaverse too soon may create confusion, weaken the meaning of those rights, and fail to protect people in practice.

4.01 The Law as a Reactive Discipline

Law, by its very nature, is a reactive discipline. It responds to social transformations after they have matured, not before. Caballero & Balbuena observe that legal systems typically adapt to technological change only once they have demonstrably impacted real people in tangible ways.[98] It is not the business of law to regulate speculative futures, but to provide structure for lived realities.[99] The Metaverse, in its current state, remains largely experimental and fragmented, with no universally accepted definition[100] and no coherent understanding of its social, political, or ethical architecture.[101]

98 Ibid no. 21.

99 Karma Dabaghi, 'Beyond design thinking and into speculative futures in legal design' in Lockton, D., Lenzi, S., Hekkert, P., Oak, A., Sádaba, J., Lloyd, P. (eds.), DRS2022: Bilbao, 25 June - 3 July, Bilbao, Spain.
<https://doi.org/10.21606/drs.2022.307 > accessed 29th July 2025

100 Ibid no. 58.

101 Simon Elias Bibri, 'The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities: A Study in Science, Technology, and Society' (2022) Smart Cities 5, no. 3: 832-874 <https://doi.org/10.3390/smartcities5030043> accessed 29th July 2025

Therefore, to develop a human rights framework around an environment that is still being constructed, both technologically and normatively, is to legislate in a vacuum. It invites legal uncertainty, overreach, and the imposition of norms that may not correspond to actual harms or lived experiences. As Lamprecht warns, the proliferation of ill-understood regulations erodes trust in legal systems and undermines their legitimacy.[102]

4.02 The Law Does Not Keep Pace

The relationship between law and technology is asymmetrical. While law may seek to guide behaviour, it is technology that is actively reshaping the conditions of that behaviour. Algorithms are already transforming not only our institutions but also our moral intuitions and social identities.[103] To presume that law can pre-emptively extend its authority into these evolving domains is naïve. Rather than shaping technology, law is often shaped by it, sometimes radically so, as with the advent of social media, surveillance capitalism, and algorithmic governance.

The extension of human rights into the Metaverse would presuppose a legal omniscience that does not exist. It would require lawmakers to predict how identity, agency, harm, and community will evolve in synthetic environments, a task that borders on the metaphysical.[104] Without a clear understanding of what it means to be a "subject" in the Metaverse, or even who qualifies as one (a user? an AI agent? an avatar?), the legal apparatus of rights risks being misapplied or rendered ineffective.[105]

4.03 Law Cannot Comprehend the Algorithmic World

The legal system is semantic and normative, while computing systems are syntactic and operational. Caballero & Balbuena argue that this distinction is more than academic, it is structural.[106] Law governs

102 Anita Lamprecht, 'Part 6: Governing the metaverse through standards' (*Diplo*, 27 March 2025) <https://www.diplomacy.edu/blog/part-6-governing-the-metaverse/ > accessed 29th July 2025

103 Ibid no. 21.

104 Diana Peña Cuellar, Astrid Vidal Lasso and Alejandra Buriticá Salazar, 'The metaverse: an analysis from a human rights perspective' (2024) Revista Jurídica Mario Alario D'Filippo, 16(33), 202-218 <https://doi.org/10.32997/2256-2796-vol.16-num.33-2024-4889 > accessed 22nd April 2025

105 The Plenary Assembly of the CNPEN, 'Opinion n°9 of the French National Pilot Committee for Digital Ethics Metaverses: ethical issues' (2024) <https://www.ccne-ethique.fr/en/publications/opinion-ndeg9-metarveses-ethical-issues> accessed 29th July 2025

106 Ibid no. 21.

meaning, context, and intention. Algorithms operate on logic, pattern recognition, and optimisation. In environments governed by code, surveillance, and AI-generated outcomes, the invocation of traditional human rights such as freedom of expression or due process becomes tenuous.[107] These rights presuppose human agency, moral reasoning, and state accountability, all of which are obscured in the Metaverse by the opacity of algorithms and the decentralisation of control.[108]

Further, applying human rights in such an environment is to ask legal norms to operate in a space where their preconditions do not exist.[109] The right to be free from arbitrary detention, for example, presumes physical coercion by an agent of the state, not a user being "banned" by a private platform's automated moderation tool. Likewise, the right to freedom of expression presumes a public forum governed by democratic norms, not a corporate server governed by terms of service.[110]

4.04 Jurisdictional Ambiguity

Unlike the territorial sovereignty that grounds human rights enforcement in the physical world, the Metaverse is a transnational digital construct. Users, platforms, and data flows often span multiple jurisdictions simultaneously. Chawki *et al.* note that this reality introduces severe enforcement dilemmas.[111] What law governs a virtual assault committed in a platform hosted in the United States (US) operated by a company incorporated in Ireland, affecting a user based in Kenya? Traditional legal tools like treaties, extradition, and national laws are not well-equipped to handle the fast, borderless nature of interactions in the Metaverse.[112]

While proposals such as an international digital treaty[113] or "electronic jurisdictions"[114] attempt to bridge this gap, they remain aspirational

107 Alan Willie, 'AI and Human Rights: Exploring the Impact of AI Technologies on Fundamental Rights such as Privacy, Freedom of Expression, and Equality' (*Stanford University*, September 2024) <https://www.researchgate.net/publication/387364266_AI_and_Human_Rights_Exploring_the_Impact_of_AI_Technologies_on_Fundamental_Rights_such_as_Privacy_Freedom_of_Expression_and_Equality> accessed 29th July 2025

108 Ibid no. 52.

109 Ibid no. 20.

110 Ibid, no. 152.

111 Ibid no. 52.

112 Ibid, no. 20.

113 Ibid, no. 52.

114 Ibid no. 51.

and logistically burdensome. Unlike states, platforms do not owe international human rights obligations unless such norms are codified and domestically enforced. Therefore, assigning duties to non-state actors like Meta raises unresolved questions about the legitimacy, capacity, and accountability of private corporations in enforcing rights-based regimes.[115]

While the impulse to extend human rights into the Metaverse stems from a legitimate concern for dignity and justice in digital spaces, the arguments presented in this section have demonstrated that such an extension may be premature and conceptually flawed. As the Metaverse remains technologically unsettled and socially undefined, attempting to apply traditional human rights frameworks risks generating more ambiguity than protection. The law, inherently reactive, struggles to regulate environments whose architecture and social dynamics are still in flux. Moreover, the unique characteristics of the Metaverse, its algorithmic governance, lack of centralised authority, and jurisdictional fluidity, challenge the foundational assumptions on which human rights law rests. Without clear subjects, enforceable duties, and stable institutions, the practical mechanisms for implementing rights become elusive. As the several scholars above caution, prematurely transplanting human rights into this context may erode legal credibility. While ethical regulation and corporate responsibility remain important, the wholesale application of rights-based regimes to the Metaverse may ultimately prove more symbolic than effective, raising the need for alternative frameworks that are better suited to the complexities of virtual life.

5.0 Why Human Rights Should Not (Yet) Be Extended into The Metaverse

5.01 Critique of the Extensionist Perspective

A closer reading of the extensionist arguments advanced in support of transplanting human rights into the Metaverse reveals several underlying assumptions that, while well-intentioned, expose significant conceptual and practical limitations. First, there is a fundamental

115 Ibid no. 65.

cf Monika Zalnieriute, 'The Necessity for Binding Human Rights Obligations for Private Actors in the Digital Age: A Submission to the UN Human Rights Council on New and Emerging Technologies' (2019) UNSW Law Research Paper No. 19-81 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470951 > accessed 29th July 2025>

assumption of legal translatability. The scholars proceed on the premise that human rights norms, originally conceived for the tangible, physical world, can be seamlessly extended into virtual environments. This position tends to overlook the distinctive philosophical and legal architecture of human rights, which are historically grounded in the corporeal presence of the rights-holder and predicated upon a clear duty-bearer, typically the state. The assumption that virtual avatars or digital environments can easily replace real human beings overlooks the foundation on which rights are built, our physical, lived existence. In this context, there is an insufficient interrogation of whether virtual entities meet the necessary criteria to generate or receive rights, particularly rights as foundational as the right to life, dignity, or bodily integrity.

Second, the extensionist argument appears to rest on an assumption of regulatory maturity. The proposal to extend human rights into the Metaverse presupposes the existence of a sufficiently harmonised global legal infrastructure, one that can recognise, monitor, and enforce those rights across decentralised, multi-jurisdictional networks. This presumption underestimates the stark disparities in digital regulatory capacity across jurisdictions, especially between the Global North and South. In jurisdictions such as Kenya, where digital infrastructure and legal capacity are still developing, the practical ability to implement such rights remains highly constrained. Moreover, the intricate nature of Web3 technologies, including Blockchain and smart contracts, further complicates any attempt to translate rights-based norms into enforceable digital governance.

Finally, the extensionist arguments offer limited guidance on enforcement. Although it gestures towards regulatory gaps and the need for platform accountability, it does not articulate a workable path for realising rights in practice. The suggestions offered remain largely ambitious, lacking concrete mechanisms for adjudication, remedy, or transnational enforcement. This shortfall renders the proposed framework vulnerable to what might be called the implementation gap, where the rhetorical promise of rights outpaces the institutional means to make them real. In such a scenario, rights risk becoming performative or symbolic rather than meaningful or effective, with no viable pathway from legal claim to material redress.

5.02 Conceptual and Legal Barriers to Human Rights in the Metaverse

The expansion of human rights into the Metaverse is rapidly emerging as a frontier legal debate, fuelled by growing concerns over digital harms, virtual economies, and evolving modes of human presence online. As discussed in previous sections, proponents advocate for an urgent transplant of rights frameworks from the physical into the virtual, arguing that immersive environments and avatars require the same legal protections traditionally afforded to corporeal individuals. Yet this enthusiasm risks outpacing legal reason, conceptual coherence, and institutional capacity. In this next section, we argue that extending human rights into the Metaverse is premature and problematic.

While the desire to safeguard dignity and justice in digital spaces is legitimate, the wholesale application of human rights law into the Metaverse is based on flawed assumptions. These include the belief that legal norms designed for state-based societies and physical embodiment can be translated seamlessly into decentralised, code-governed systems.[116] Drawing from a range of scholarly contributions, we challenge the notion that avatars or code-based interactions meet the jurisprudential thresholds necessary to trigger human rights protections. We also examine the limitations of enforcement, the problem of duty-bearers, the asymmetry between law and technology, and the risk of normative inflation. Throughout, we adopt a globally reflective lens while referencing examples from Kenya.

5.03 The Problem of Duty Bearers

Human rights law is traditionally underpinned by a binary structure: rights holders and duty bearers.[117] Individuals are entitled to protections, and states bear the responsibility of enforcement. The Metaverse, however, collapses this structure. In decentralised environments, it is not clear who can or should be held accountable for upholding rights. Is it the platform provider, the algorithm designer, or the user behind the avatar?

116 Ibid, no. 20.

cf Diana Peña Cuellar, Astrid Vidal Lasso and Alejandra Buriticá Salazar, 'The metaverse: an analysis from a human rights perspective' (2024) Revista Jurídica Mario Alario D'Filippo, 16(33), 202-218 <https://doi.org/10.32997/2256-2796-vol.16-num.33-2024-4889 > accessed 22nd April 2025

117 Simret Natnael Goitom, 'Filling the Gaps in the Right to Development A Study on the Understandings (and Misunderstandings) of Rights-Holders and Duty-Bearers' (2013) Lund University Publications <https://www.lunduniversity.lu.se/lup/publication/3802939> accessed 29th July 2025

Chawki *et al.* identify a core obstacle: the anonymity and decentralisation inherent in Web3 architectures like the Metaverse, which thwart traditional enforcement.[118] Decentralised platforms may not even have a legal entity to hold accountable. Worse still, such structures invite regulatory arbitrage, whereby malicious actors exploit legal gaps without consequence. The lack of a centralised locus of responsibility renders conventional human rights protections not just difficult to enforce, but structurally incompatible with the environment in which violations would allegedly occur. Moreover, efforts to assign human rights duties to private platforms raise serious concerns about legitimacy and capacity.[119] As non-state actors, these entities are not treaty parties and do not possess the sovereignty required to fulfil constitutional obligations. Imposing such burdens may also distort their roles, transforming terms-of-service agreements into quasi-constitutional charters, a mismatch that threatens to stifle innovation without delivering meaningful justice.

5.04 Human Rights and the Nature of the Metaverse

Caballero and Balbuena state that law is a semantic and reactive construct, while technology, particularly code, is syntactic.[120] Human rights are grounded in the moral reality of embodied human subjects, not algorithmic agents. The moral claims that justify rights, such as bodily vulnerability, emotional sentience, and autonomous personhood, are absent in avatars, or synthetic environments.[121]

To transpose the "right to life" or "freedom from inhuman treatment" into a realm where harm is simulated or disembodied is not merely abstract; it is conceptually illogical. What does it mean, legally or morally, to violate the dignity of an avatar? Can the deletion of a digital persona be likened to homicide?[122] These analogies stretch jurisprudence into a metaphysical terrain it is ill-equipped to navigate.

Furthermore, avatars lack the biological fragility that grounds many rights protections. While a user may feel distress if their avatar is

118 Ibid, no. 52.
119 Ibid, no. 65.
120 Ibid, no. 21.
121 Ibid, no. 51.
122 Caesar Kalinowski IV, 'Is It Really Murder If the Victim Lives on in a Digital Form?' (*The Legal Geeks*, 21 June 2018) <https://thelegalgeeks.com/2018/06/21/is-it-really-murder-if-the-victim-lives-on-in-a-digital-form/> accessed 30th July 2025

attacked or defaced, the harm remains psychological and symbolic rather than physical and direct.[123] This does not mean the harm is insignificant, but it does raise questions about whether it falls within the domain of human rights or instead requires a new category of digital protections grounded in ethics and platform governance.

5.05 Legal and Institutional Constraints on Enforcement

Even if conceptual thresholds were resolved, practical limitations remain. Enforcement of rights in the Metaverse is fraught with jurisdictional ambiguity and evidentiary gaps. Virtual spaces are inherently transnational, with users, servers, and data flows distributed across multiple legal regimes.[124] Traditional tools like mutual legal assistance treaties, extradition frameworks, and domestic cybercrime laws are ill-suited to this context.

Attempts to address these challenges through proposals such as "electronic jurisdictions"[125] or digital rights treaties.[126] They are ambitious and legally infeasible. Without harmonised standards or transnational enforcement mechanisms, rights enforcement becomes symbolic rather than substantive. Assigning obligations to private actors like Meta may offer a stopgap, but without legal compulsion or oversight, such measures depend on corporate goodwill, a fragile foundation for fundamental rights.

This problem is particularly pronounced in low- and middle-income jurisdictions, where enforcement capacities are already strained in the physical realm. For example, while Kenya's *Data Protection Act, 2019*[127] and the *Computer Misuse and Cybercrimes Act, No. 5 of 2018*[128] provide comprehensive frameworks for addressing online harms, extending their remit into the Metaverse, especially across decentralised networks, would stretch resources thin and compromise enforcement efficacy.

123 Mark Alan Graber and Abraham David Graber, 'Get Your Paws off of My Pixels: Personal Identity and Avatars as Self' (2010) J Med Internet Res 2010;12(3): e28 <https://www.jmir.org/2010/3/e28/> accessed 30th July 2025

124 Ibid, no. 52.

125 Ibid, no. 51.

126 Tore Tennøe and Adele Matheson Mestad 'The Metaverse and Human Rights' (*Norwegian Human Rights Institution*, 5 December 2022) <https://www.nhri.no/en/report/the-metaverse-and-human-rights/?showall=true> accessed 20th April 2025

127 Data Protection Act, 2019

128 Computer Misuse and Cybercrimes Act, No. 5 of 2018

5.06 Asymmetry Between Law and Technology

A recurring theme in contemporary scholarship is the fundamental asymmetry between legal frameworks and technological innovation. As stated above, law is by its nature reactive, meaning it responds to concrete harms rather than speculative possibilities. Caballero and Balbuena explain that legal structures evolve slowly and in response to socially recognised injuries, whereas digital technologies evolve generatively, reshaping environments with little warning.[129] To presume that law can pre-emptively regulate emergent virtual environments is to attribute to it a predictive capacity it does not possess. Yet this is not simply a question of legislative delay. It reflects a deeper structural divide. Law and code operate on fundamentally different planes. Legal norms are interpretive, contextual, and human-centred. Code is rigid and indifferent to morality.[130] The challenge becomes particularly acute when one attempts to embed legal principles, especially human rights, into algorithmic governance systems. This translation presumes that legal standards such as "justifiable limitations" under *Article 24 of Kenya's Constitution* can be rendered into fixed, programmable rules. But such provisions require nuance, discretion, and the balancing of competing interests, none of which can be meaningfully encoded in binary logic.

Further, this philosophical misalignment is made inadequate by the rapid pace of technological change. Technologies like Blockchain, generative AI, and mixed-reality platforms are evolving faster than even the most adaptable legal systems can keep up with.[131] Writing human rights directly into code would require a level of foresight that neither lawmakers nor technologists currently have. Algorithms increasingly shape how people interact with the world, but they do so by processing data and optimizing patterns, not by applying values like dignity or justice.

The above challenges are not merely hypothetical. They create real problems for legal procedures and enforcement. In the Metaverse, digital identities are often temporary, pseudonymous, and easily deleted. While transactions may be recorded, evidence can vanish instantly, and peer-to-peer systems often resist centralized control. It

129 Ibid, no. 21.
130 Ibid, no. 21.
131 Ibid, no. 21.

has been suggested that transaction records should be preserved for accountability,[132] but even the best-kept logs do not always link back to real people. In this setting, applying constitutional rights, like Kenya's guarantee of a fair hearing under *Article 50 of the Constitution*, becomes difficult. Such rights assume that individuals are identifiable, have legal standing, and that duties can be enforced. Virtual pseudo-anonymity and decentralized platforms challenge all these assumptions.

Further complications arise when we try to place human rights duties on private entities like platforms or developers. States are the proper enforcers of constitutional rights because they have legal authority and are bound by public accountability.[133] In contrast, private companies operate through contracts and commercial goals.[134] Expecting them to uphold state-level human rights through their terms of service misplaces responsibility and blurs the line between public and private law. This could weaken accountability and discourage innovation, especially in countries trying to become leaders in digital development.

Altogether, these problems highlight a key point: although extending human rights into the Metaverse may seem appealing, it is built on a misalliance of ideas and practical limitations. Instead of forcing traditional legal frameworks into virtual spaces where they do not fit, it would be wiser to develop tailored or bespoke regulatory tools. These should focus on ethical design, fair procedures, and digital accountability, principles that respond to the unique features of virtual environments without stretching the human rights framework beyond its intended scope.

5.07 Risk of Normative Inflation and Dilution

The authors further contend that perhaps the most profound danger of extending human rights into the Metaverse lies in the dilution of their normative force.[135] Human rights gain their legitimacy from well-defined moral principles and a deep historical legacy. They are designed to safeguard life, liberty, equality, and dignity, not to address every digital inconvenience or avatar deletion, in a digital forum. If

132 Ibid, no. 52.

133 Danwood Mzikenge Chirwa, The Doctrine of State Responsibility as A Potential Means of Holding Private Actors Accountable for Human Rights. (2004). Melbourne Law School <https://search.informit.org/doi/10.3316/agispt.20044710> accessed 30th July 2025

134 Ibid no. 65.

135 Ibid, no. 20.

every avatar ban, NFT scam, or minor platform dispute is elevated to the level of a constitutional grievance, the term "human rights" risks becoming inflated, trivialised, and detached from its original moral and legal foundations.

Lamprecht cautions that such overextension erodes public trust in legal systems and invites judicial overreach.[136] Courts may increasingly find themselves adjudicating marginal or speculative claims under the banner of fundamental rights, weakening the coherence, utility, and legitimacy of the rights discourse itself. A proliferation of Metaverse-based rights claims, and the absence of corresponding enforcement mechanisms would not only clog the judicial system but render the language of rights meaningless.

Moreover, extending human rights wholesale into the Metaverse risks severing those protections from the very human experiences they are meant to safeguard. At the root, human rights presuppose an embodied moral subject, an individual whose dignity, autonomy, and security depend on the integrity of the body and its surrounding social context.[137] While avatars may simulate presence, they lack the vulnerability, sentience, and moral agency that ground human rights in the physical world.[138] To ascribe a "right to life" to a digital representation is to conflate the lived reality of a person with lines of code, a conceptual leap that trivialises both the right itself and the human being it is meant to protect. This lack of philosophical and legal consistency not only weakens the clear meaning of rights but also risks making them meaningless in both the digital and physical worlds.

5.08 Equity and Access

A further consequence of premature rights expansion is that it could worsen existing digital inequality. Lamprecht notes that even legal professionals in well-resourced jurisdictions struggle to keep pace with emergent technologies.[139] For many in the Global South, legal literacy, digital infrastructure, and institutional capacity remain

136 Ibid no. 102.

137 Talal Agil Attas Alkhiri, '*Human Right Requirements in the Metaverse Era*' (2022) International Journal of Computer Science and Network Security (IJCSNS), Vol. 22 No. 8 <https://doi.org/10.22937/IJCSNS.2022.22.8.9> accessed 20th April 2025

138 Ibid, no. 51.

139 Ibid no. 102.

underdeveloped. To introduce a Metaverse-specific rights regime in such settings risks creating a parallel system accessible only to the wealthy, the connected, and the technologically literate.[140] Rights would become a digital luxury rather than a universal guarantee. In this context, virtual protections may end up reinforcing rather than redressing systemic injustice.

Take, for example, a hypothetical claim of avatar "defamation" brought before the High Court. Without clear procedural rules, jurisdictional clarity, or evidentiary standards, the court may either dismiss the claim as frivolous or struggle to adjudicate it using analogies from the physical world. In either case, legal certainty is compromised.

5.09 Regulation Without Rights Transposition

Acknowledging these challenges does not amount to ignoring the real harms that occur in digital environments. Virtual fraud, harassment, exploitation, and manipulation are serious and growing problems. But their solution lies not in the wholesale transplantation of human rights law into virtual space, but in the development of bespoke regulatory and ethical frameworks.

Jurisdictions like Kenya should prioritize expanding existing cybercrime statutes, strengthening data protection laws, and creating new legal categories for digital harms that fall outside the traditional rights framework, instead of declaring a new generation of Metaverse rights. Also, regulatory sandboxes, platform governance codes, and international best practices are tools that can help fill the gap without distorting the meaning of rights.[141]

As an illustrative example, Kenya could develop a "Metaverse Charter" under the Communications Authority of Kenya, akin to the National ICT Policy Framework,[142] that outlines principles of digital fairness, transparency, and accountability without invoking constitutional language. Such a charter could draw from interdisciplinary sources, cyberlaw, ethics, and behavioural science, while respecting the

140 Ibid, no. 52.

141 Ibid, no. 20.

142 Ministry of Information, Communications and Technology, 'National ICT Policy' (2020) <https://ke-cirt.go.ke/wp-content/uploads/2021/07/NATIONAL-ICT-POLICY-2019.pdf> accessed 30th July 2025

boundary between enforceable rights and aspirational standards.[143]

5.10 Jurisdictional Fragmentation

A critical obstacle to the effective extension of human rights into the Metaverse lies in the jurisdictional disarray that defines this emerging digital frontier. The Metaverse is inherently transnational, decentralised largely due to Blockchain technology, and structurally resistant to traditional forms of state control.[144] Its architecture, comprising decentralised autonomous organisations (DAOs), peer-to-peer protocols, and self-executing smart contracts, does not align with the territorial foundations of state-based legal enforcement. As a result, the enforcement of human rights, which presumes identifiable duty bearers within a defined jurisdiction, becomes not only impractical but conceptually incoherent.

Kenya offers a particularly illustrative example of this dilemma. Even with forward-looking legislation such as the *Computer Misuse and Cybercrimes Act No. 5 of 2018* and the *Data Protection Act, 2019*, Kenya remains constrained by the territorial limits of its jurisdiction. The country simply cannot compel compliance from platforms hosted on servers in Singapore, governed by developers in Estonia, or built on decentralised Blockchains that defy national oversight altogether. If a Kenyan citizen suffers a virtual assault or economic harm in the Metaverse, for example, through the unauthorised sale of virtual land on a Blockchain-based platform like Decentraland, it is far from clear which legal system would apply, which authority would have stood, and who would bear the burden of redress.

Although Kenya's Internet Governance Forum (KeIGF) has demonstrated the potential of multi-stakeholder engagement in shaping national and regional digital policy, such collaborative models[145] are still embryonic when it comes to the Metaverse. They lack the legal force and institutional architecture required to resolve complex transboundary disputes, particularly where competing laws,

143 Dr. Maria O'Sullivan, 'Human Rights in the Metaverse – Digital Nations, Political Participation and Protest' (*ALTI*, 1 October 2024) <https://alti.amsterdam/human-rights-in-the-metaverse/> accessed 22nd April 2025

144 Thien Huynh-The, Thippa Reddy Gadekallu, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa and Madhusanka Liyanage, 'Blockchain for the metaverse: A Review' (2023) Future Generation Computer Systems, Volume 143, Pages 401-419 <https://doi.org/10.1016/j.future.2023.02.008> accessed 30th July 2025

145 Kenya Internet Governance Forum <https://kigf.or.ke/> accessed 30th July 2025

absent treaties, and inconsistent enforcement mechanisms prevail. As it stands, we do not believe that there is an existing binding international legal instrument that could adequately address the governance of decentralised digital ecosystems. Efforts to harmonise legal standards, through initiatives like the African Union's Digital Transformation Strategy[146] or the Council of Europe's work on AI and human rights,[147] remain fragmented, non-binding, or largely symbolic.

The consequence is a legal vacuum in which rights claims are likely to splinter across multiple, and often conflicting, jurisdictions. Victims of digital harm may be left without effective recourse, and violators may exploit gaps in oversight through regulatory arbitrage. Worse still, this mismatch could invite false expectations, where individuals invoke rights protections without any real prospect of enforcement, undermining trust in both digital platforms and state institutions.

This legal fragmentation is a procedural inconvenience that strikes at the heart of what it means to guarantee justice. If human rights are to remain meaningful, they must be enforceable. In the Metaverse, without a global legal framework, it becomes nearly impossible to enforce rules because different jurisdictions clash and create confusion. Thus, extending human rights into this space without first resolving the governance question is not only premature, but it risks turning rights into empty words that have no real legal power or practical support and institutional capacity.

5.11 Limitations and Assumptions

The authors of this article argue that extending traditional human rights frameworks into the Metaverse is conceptually and practically flawed. Central to their position is the assumption that human rights obligations can only be enforced by states. This state-centric model excludes private actors, such as decentralised platforms or developers, from serving as legitimate duty-bearers. However, this view overlooks how domestic legal systems already impose human rights-like responsibilities on private entities through data protection, employment, and anti-discrimination laws. Moreover, it

146 African Union, 'The Digital Transformation Strategy for Africa (2020-2030)' *(African Union*, 18 May 2020) <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030> accessed 30th July 2025

147 Council of Europe, 'Artificial intelligence and human rights' (2025) <https://www.coe.int/en/web/artificial-intelligence> accessed 30th July 2025

underestimates the potential for hybrid governance models, where corporate platforms voluntarily adopt enforceable rights-like standards through regulation or contractual obligations.

Another key assumption is that only physically embodied persons can claim rights, dismissing avatars as morally and legally irrelevant. Yet this anthropocentric view ignores the fact that real users can suffer tangible emotional or economic harm in virtual spaces. Legal systems already recognise intangible injuries (e.g., defamation, privacy breaches), suggesting the possibility of extending certain protections to digital personas without distorting the core of human rights.

Enforcement is also portrayed as infeasible due to jurisdictional fragmentation and technological anonymity. While cross-border enforcement is complex, the authors assume that a global legal vacuum cannot be effectively addressed. Extraterritorial jurisdiction, regulatory cooperation, and emerging regional frameworks (e.g., the African Union's digital strategy) offer viable pathways for oversight.

Another assumption concerns how legal rules operate in technological contexts. The authors emphasize a "fundamental asymmetry" between law and technology: law is "interpretive, contextual, and human-centred" while code is "rigid and indifferent to morality". They argue this gap makes it impossible to encode detailed or context-sensitive rights protections into programmable form. The underlying premise is that legal principles inherently demand human judgment and cannot be captured by algorithms. By extension, they imply that any attempt to bake human rights values (dignity, fairness) into the Metaverse platform rules is doomed to fail.

This view correctly highlights a real challenge that legal concepts often require discretion. However, it assumes that code must be entirely binary and static. In fact, algorithmic systems can be designed with sophisticated rulesets, machine learning, and human oversight to approximate complex and context-aware outcomes (for instance, content moderation algorithms trained to respect privacy standards). The distinction between code and law may not be absolute. In regulatory practice, legislators sometimes adopt broad, principle-based rules that can be implemented in automated ways (e.g. automated

privacy compliance tools).[148]

Finally, the authors warn of "rights inflation" that extending rights to digital inconveniences trivialises them. While the concern is valid, it assumes digital harms are inherently minor, overlooking how some virtual conduct (e.g., harassment or fraud) can cause serious harm. Overall, their approach, while cautionary, may be overly rigid in dismissing the law's capacity to adapt.

6.0 Alternatives to Extending Human Rights into The Metaverse

Having established the conceptual and practical limits of extending traditional human rights into the Metaverse, it becomes essential to articulate alternative pathways, ones that do not abandon the spirit of human rights but rather reimagine their expression through context-sensitive, enforceable, and intellectually coherent regulatory strategies. In what follows, we propose a set of regulatory tools that collectively respect human dignity and agency in virtual spaces without importing the full weight of a constitutional framework ill-suited to a digital frontier.

To begin with, the principle of digital constitutionalism presents a compelling meta-governance model. Instead of force-fitting rights designed for tangible, state-governed environments into digitally native, decentralised spaces, digital constitutionalism acknowledges the *sui generis* character of the virtual realm. As the OECD has observed, countries like Italy, Portugal, Spain, Brazil, and Chile (notably with its constitutional recognition of neuro-rights).[149] They are already experimenting with digital rights charters that enshrine principles such as transparency, accountability, due process, and user autonomy.[150] These frameworks are not mere replicas of analogue legal systems. They respond directly to the vulnerabilities and asymmetries of digital life, including platform governance, algorithmic bias, and the erosion of informed consent.

Crucially, such constitutionalism does not rely solely on state action. Platforms, increasingly acting as quasi-public spheres, must assume procedural obligations akin to those of public institutions. Governance becomes a form of shared stewardship that is democratically structured, procedurally fair, and

148 Gerard Buckley, Tristan Caulfield and Ingolf Becker, 'How might the GDPR evolve? A question of politics, pace and punishment' (2024) Computer Law & Security Review, Volume 54, 106033 <https://doi.org/10.1016/j.clsr.2024.106033> accessed 30th July 2025

149 OECD, 'Rights in the digital age – Challenges and ways forward' (*OECD Digital Economy Papers No. 347,* December 2022) <https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf> accessed 30th July 2025

150 Ibid, no. 149.

rooted in community participation. This is particularly relevant in jurisdictions experimenting with digital transformation, but where regulatory capacity remains under development. For such countries, a digital charter can serve as both governance prototype and scaffolding for future norm-setting.

Second, the need for contextual and layered regulation cannot be overstated. The decentralised, borderless nature of the Metaverse renders conventional legal tools blunt and often inapplicable. Instead of relying solely on binding international law, we propose a hybrid regime grounded in soft law, such as codes of conduct, ethical standards, and technical design protocols, that can evolve in step with technological advancements. Robertson highlights that many platform harms originate not from malice but from negligent design.[151] As Meta's Human Rights Director, Miranda Sissons, aptly notes, "You have to educate and train engineers, marketing teams, etc., on the importance of human rights and the consequences of their product to society."[152] In short, the path to meaningful digital rights begins not in courtrooms, but in codebases.

Third, the development of a Metaverse-specific legal code offers an elegant and coherent alternative to the transplantation of constitutional rights. Cheong has proposed a modular legal architecture composed of a Metaverse Constitution, Criminal Code, and Electronic Chancery.[153] He also presents another viewpoint that resists the personification of avatars or granting them legal subjecthood and instead recommends service-based regulation analogous to that applied in telecommunications or e-commerce law.[154]

This bespoke approach achieves four aims. First, it avoids anthropomorphising code-based entities and preserves the integrity of the rights discourse. Second, it creates actionable legal categories like virtual harassment, identity fraud, and avatar impersonation, specifically tailored to immersive environments. Third, it reinforces platform accountability without conflating corporate compliance with sovereign duty. And finally, it saves courts from the difficult task of trying to compare virtual actions to real-world ones.

Importantly, many jurisdictions already possess legal instruments capable of addressing these harms. Preserving legal coherence through existing law**,** rather than proliferating new categories of digital rights, offers a pragmatic and legally minimalist solution. For example, the *Computer Misuse and Cybercrimes*

151 Derek Robertson, 'Human rights in the metaverse' (*Politico*, 6 July 2022) <https://www.politico.com/newsletters/digital-future-daily/2022/06/07/human-rights-in-the-metaverse-00037853> accessed 22nd April 2025

152 Ibid, no. 149.

153 Ibid, no. 51.

154 Ibid, no. 149.

Act No. 5 of 2018 already penalises offences such as cyberbullying and the dissemination of offensive material. Similarly, the constitution itself, consumer protection, intellectual property, and data protection laws can be expanded, through legislative clarification or case law, to encompass virtual experiences.

International cooperation also remains critical. The Budapest Convention on Cybercrime[155], which Kenya is actively aligning with, sets a precedent for transnational enforcement mechanisms. Instead of conjuring new rights regimes, we ought to focus resources on strengthening these enforcement pathways, improving cross-border collaboration, and investing in digital literacy to ensure meaningful access to remedies.

Lastly, jurisdictions such as Kenya are uniquely placed to pioneer regulatory innovation in the governance of immersive digital spaces. With its dynamic tech sector, progressive constitutional framework, and growing digital infrastructure, Kenya has both the legal foundations and policy appetite to develop a context-sensitive model for Metaverse governance. A "Kenya Metaverse Charter" could serve as a forward-looking template grounded in constitutional values like dignity, equality, and participatory democracy, for managing virtual platforms in a manner that is transparent and rights-conscious.

Such a charter could institutionalise participatory rulemaking through structured public consultations, ensuring that platform governance reflects the lived experiences and concerns of Kenyan users. It could also establish independent oversight mechanisms to monitor compliance and accountability, particularly in areas such as data protection, digital safety, and algorithmic fairness. Civic education initiatives would further enhance digital literacy, equipping citizens especially the youth, with the knowledge needed to navigate virtual environments safely and assert their digital rights effectively.

Kenya need not wait for a global treaty or uniform consensus to take meaningful action. Through the development of bespoke regulatory frameworks that balance technological innovation with ethical safeguards, Kenya can assert itself as a leader in shaping responsible digital futures. This forward-leaning approach would not only safeguard national interests but also elevate Kenya's standing as a thought leader in the Global South, contributing constructively to international conversations on digital governance while laying the groundwork for a dignified, adaptive, and contextually relevant engagement with the Metaverse.

155 Council of Europe, 'The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols' <https://www.coe.int/en/web/cybercrime/the-budapest-convention> accessed 30th July 2025

7.0 Conclusion

The article contends that the question of extending human rights into the Metaverse is not simply a matter of legal interpretation or technical design; it is a profound conceptual challenge. Human rights, as historically conceived, rest on assumptions of embodied personhood, state accountability, and territorial jurisdiction. These foundations begin to unravel in decentralised, pseudonymous, and algorithmically governed virtual environments. To apply the traditional rights framework wholesale to such spaces risks not only legal incoherence and enforcement paralysis, but also the dilution of the very normative force that gives human rights their legitimacy. In the process, we may trivialise the moral seriousness of rights and stretch legal systems beyond their institutional capacities.

Still, this critique should not be misunderstood as a call for regulatory inertia. On the contrary, protecting human dignity, autonomy, and equality in virtual spaces remains an urgent imperative. But doing so requires a shift in legal imagination from transposing existing rights to constructing new regulatory architectures. This article has advocated a pluralistic, layered approach, drawing from soft law instruments, platform governance, digital constitutionalism, and bespoke Metaverse-specific legal codes. These mechanisms can offer real safeguards without the burden of fitting novel harms into frameworks that were not designed for them.

Kenya, alongside other digital-forward jurisdictions in the Global South, is well-positioned to pioneer such an approach. A Kenya Metaverse Charter grounded in public consultation, ethical design, and independent oversight could serve as a model for adaptive, participatory governance in virtual worlds. Kenya need not wait for a global treaty or defer to external norms; it can chart its own regulatory future, one that aligns innovation with dignity, and digital transformation with democratic values.

Ultimately, the question is not whether law should govern the Metaverse, but how. As the authors have argued, the answer lies not in legal inflation but in principled legal evolution. Human rights must remain resilient but also responsive. To safeguard their coherence, we must be willing to say: not yet here, not in this form. Rights are too valuable to be applied indiscriminately, particularly in the boundless terrains of the Metaverse.

LSK REGULATED N-WDT SACCO SOCIETY LTD

JOIN US TODAY

Membership is open to:

- ☑ Members of the Law Society of Kenya, their spouses, children and permanent employees.
- ☑ Employees of institutions within the administration of justice.

BENEFITS

- ☑ Competitive annual interest on deposits and dividends
- ☑ Investment advice through members education seminars
- ☑ Loans to a maximum of Kes 40M (Forty Million)
- ☑ Loans at lower interest rate 1% per month on reducing balance.
- ☑ Flexibility in loan repayment of up to 14yrs
- ☑ Flexible loan security options (Guarantors, Title deeds, Motor vehicle, Self-guarantee)
- ☑ Quick loan approval and Loan disbursement.

LOAN PRODUCTS

- ☑ Development loan (House/Land, Car & Business financing)
- ☑ Emergency Loan
- ☑ Education Loan
- ☑ Vuka Loan
- ☑ Refinancing loan

SAVINGS

- ☑ Sacco shares (Non-refundable but transferable) -earns dividends annually- (12% as of year 2024)
- ☑ Sacco deposits/Savings – earns interest annually (9.5% as of year 2024)
- ☑ Holiday Savings
- ☑ Children Savings

Secure your holiday home with a 100x100 plot at the LSK Housing Wakili Palm Project in Diani. Learn more about the project here: https://lskhousing.co.ke/wpv

LSK HOUSING CO-OP SOCIETY LIMITED

www.lsksacco.co.ke | 020-514 6300 : 0717113134| info@lsksacco.co.ke|LSK SACCO:

Governing Fair Play: Surveillance, Anti-Doping Regimes, and Human Rights in the Global South

*Damaris Ogama**

Abstract

This article critically questions the use of invasive digital surveillance in the global anti-doping regime and its uneven effects on athletes from the Global South. Although the World Anti-Doping Agency (WADA) advocates a harmonized system to support the integrity of sport, the available means, otherwise known as the Athlete Biological Passport, ADAMS data platform, and 24/7 geolocation monitoring, often ignore the possibility of legal plurality, the concept of informed consent, and data sovereignty. The paper discusses the reproduction of structural inequality and regulatory colonialism in these mechanisms based on a multidisciplinary perspective rooted in international human rights law, data ethics, and global governance. Drawing from studies in Kenya, Nigeria, India, and Jamaica, it demonstrates the built-in exclusion of legal illiterate, unrepresented athletes without digital access or no access to an institution or an institutionally supported constituent. The review reflects a two-tiered system where athletes in the Global North enjoy the presence of a powerful legal infrastructure, whereas athletes in the South are exposed to clouded, pressuring, and many situations, unaccountable structures. The article proposes a rebalance of anti-doping governance in terms of international standards of due process, privacy, and digital dignity. These recommendations comprise the creation of a WADA Charter of Digital Rights; consistency of data laws at the regional level; athlete-controlled support systems of athletes; and separate monitoring systems. The results explain why there is an immediate necessity for an anti-doping system, which balances sports fairness versus equality of rights.

Keywords: *Anti-doping, Privacy rights, Data protection, Human rights, Global South*

1.0 Introduction

The efforts to combat doping have become a system characterized by more and more data-driven and more surveillance-based forms, and the World Anti-Doping Agency (WADA) is at the center of this development.[1] Formed in

1 *Dr. Damaris Ogama is a Deputy Chief State Counsel at the Office of the Attorney General and Department of Justice, Kenya, and a researcher in anti-doping and sports integrity. She holds a PhD

1999 after a series of scandals cast doubt on elite sport, WADA now manages an integrated regulatory system, the World Anti-Doping Code, to expose, deter and punish doping on a global basis.[2] At the heart of this model are the application of sophisticated data collection instruments and supervisory techniques that are directed towards athletes, whether on the field or off-field.[3] Such measures entail the Athlete Biological Passport (ABP), a mechanism that monitors longitudinal blood biomarkers to detect doping indirectly; the so-called whereabouts regime, including the obligation to inform about the location daily in order to undergo possible on-notice testing; as well as random sampling procedures aimed at making enforcement unpredictable.[4] Although such mechanisms work to achieve equity and the fitness of the athlete, they have also raised complicated ethical and legal questions- especially on data protection, consent, and surveillance. Such issues are even more crucial in places with poorly developed data governance frameworks, which raises a crucial question of equity, digital rights, and an uneven athlete burden where it exists across the world.

The global anti-doping system is developed in a geopolitical climate where the promotion of regulatory commonality tends to bias the development of the concept and practice of equity in various regions.[5] Scholars have criticized the model of global governance by WADA as a duplication of asymmetrical power relations through the enforcement of rules, which are designed in the Global North with little consultation or cultural adjustments to interests in the Global South.[6] Such one-size-fits-all thinking tends to conceal the infrastructural and historical disparity that determines the experiences of athletes, like low access to the law, informational literacy, or professional representation.[7] Additionally,

in Development Studies and works at the intersection of law, public health, and clean sport governance Ivan Waddington, 'Surveillance and Control in Sport: A Sociologist Looks at the WADA Whereabouts System' (2010) 2 International Journal of Sport Policy and Politics 255

2 Roxanne Caron, *Are the Current World Anti-Doping Agency Guidelines Morally Justifiable? An Overview of Ethical Considerations and Possible Alternatives* (McGill University (Canada) 2016) <https://search.proquest.com/openview/8de223d2e4fbaad93dbd7e33ddacbb6d/1?pq-origsite=gscholar&cbl=18750&diss=y> accessed 29 July 2025

3 Waddington (n 1)

4 Dora Dragčević, Vlatka Pandžić Jakšić and Ozren Jakšić, 'Athlete Biological Passport: Longitudinal Biomarkers and Statistics in the Fight against Doping' (2024) 75 Archives of Industrial Hygiene and Toxicology 24; WADA, 'World Anti-Doping Code' (World Anti-Doping Agency 2021) <https://www.wada-ama.org/sites/default/files/resources/files/2021_wada_code.pdf> accessed 29 July 2025

5 Lorenzo Casini, 'Global Hybrid Public-Private Bodies: The World Anti-Doping Agency (WADA)' (2009) 6 International Organizations Law Review 421

6 Casini (n 5)

7 Simran Kaur Sethi, 'They Arrive, They Compete, But What's Next?: Exploring the Transition Out of Sport Experiences of Former Division I International College Athletes' <https://shareok.org/handle/11244/340275> accessed 29 July 2025

the implementation and structure of such surveillance mechanisms as the whereabouts regime are disproportionately affecting people residing in low-income countries where connectivity technology is irregular and there is low regulation.[8] This leads to a system where compliance can be frequently confused with fairness, even though it is seen that practices of enforcement are found to be insensitive to the surrounding context, and they may create procedural injustices. Indeed, the anti-doping policy has equal parts to do with sport regulation as a whole, as it does with regulations of a colonialist nature in which regulation takes place so often when the Global South can be regarded as the subject of governance rather than a counterpart.[9] It is important to interrogate the conclusion that the current anti-doping systems are not, in fact, in support of global sports integrity by recognizing the imbalance in structure.

This article examines to what degree the modern-day methods of data collection, when applied to anti-doping specifically, the use of geolocation tracking, biological surveillance, and random sampling, undermine the privacy and digital rights of the Global South athletes. Although the international anti-doping system operates on the foundations of fairness, transparency, and athlete welfare, its practical practice is becoming more dependent on comprehensive data surveillance systems, which are not always within the domain of equal relationship with national legal security, especially in low- and middle-income countries. The rules of athletics protect players in their categories with a well-established system of data protection, leaving the others with little or no protective oversight to observe without prior consent and without legal recourse and a clear understanding of their data concerning how it is stored, exchanged, and secured. This is both a regulatory and non-technical problem, but also a matter of acute human rights and an international and digital form of injustice at the intersections of global sports regulation, digital justice and postcolonial inequality. The critical analysis of structural asymmetries in the practice of administering anti-doping supervision reveals the necessity to rethink the current practices and frameworks focused on the need to guarantee that the interest in clean sport would not disregard the established systemic inequality or undermine the core rights.

8 Antoine Duval, 'The Russian Doping Scandal at the Court of Arbitration for Sport: Lessons for the World Anti-Doping System' (2017) 16 The International Sports Law Journal 177

9 Eric L Windholz, 'Sports' Global Anti-Doping Regulatory Regime: The Challenges and Tensions of Polycentricity and Hybridity' (2022) 34 Bond Law Review. 93

2.0 The Anti-Doping Regime and Digital Data Practices

WADA has a central digital platform, known as the Anti-Doping Administration and Management System (ADAMS), where the global anti-doping effort is managed.[10] ADAMS stores sensitive information about the athletes; it was designed to allow the coordination of testing, management of results, and therapeutic use exemptions. It facilitates the sharing of data in real-time between national anti-doping organizations (NADOs), laboratories, and international federations.[11] A variety of personal information is stored in this system, such as doping control forms, biological samples, medical records, and sanction histories.[12] Although integration makes it much easier to work, even the integration between two companies can attract scholarly criticism due to its lack of transparency, user control, and even jurisdictional intrusion, all of which become more concerning when data is moved across borders, with a variable level of protective treatment.[13] Such risks are especially acute in states where there are no effective laws on the protection of data, as well as the mechanisms of control. Thus, the ADAMS application evokes some unresolved conflicts between the harmonization of sport across the world and local interpretations of privacy and digital rights.

National sovereignty is frequently superseded by the functioning of the centralized data architecture of WADA, resulting in unresolvable tensions within international data governance information.[14] Depending on the strength of the constitutional protections of the right to privacy and other conflicting norms in a given jurisdiction, where there are robust constitutional privacy protections or conflictual legal standards, such as the Kenya 2019 Data Protection Act or Brazil's Lei Geral de Proteção de Dados.[15] However,

10 Flavio Pinto, 'Investigations of Blockchain Technology for Anti-Doping Data Management' (PhD Thesis, Loughborough University 2024) <https://repository.lboro.ac.uk/articles/thesis/Investigations_of_blockchain_technology_for_anti-doping_data_management/27953784> accessed 20 July 2025

11 WADA (n 4).

12 Umut Bastufek and Tineke Broer, 'Detecting the Differences of EU and WADA Limitations on the Right to Protection of Personal Data and the Implications of These Differences in National Anti-Doping Urine and Blood Screenings' <http://arno.uvt.nl/show.cgi?fid=151586> accessed 30 July 2025.

13 Diane Valkenburg, Olivier De Hon and Ivo Van Hilvoorde, 'Doping Control, Providing Whereabouts and the Importance of Privacy for Elite Athletes' (2014) 25 International journal of drug policy 212; Martin Hardie, 'Making Visible the Invisible Act of Doping' (2014) 27 International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique 85; John Gleaves and Ask Vest Christiansen, 'Athletes' Perspectives on WADA and the Code: A Review and Analysis' (2019) 11 International Journal of Sport Policy and Politics 341.

14 Pinto (n 10).

15 Sonia Livingstone and others, 'The Best Interests of the Child in the Digital Environment' <https://eprints.lse.ac.uk/122492/3/Best_Interests_of_the_Child_FINAL.pdf> accessed 30 July 2025.

in jurisdictions with strong constitutional privacy protection or where there is conflict between the law, WADA practices may conceivably constitute extraterritorial overreach.[16] The absence of a common procedure of mutual legal assistance in data requests and transfers creates legal grey areas in which data processing of athletes is done outside of the reach of domestic remedies. Most under-resourced countries do not have the technical knowledge or political will to confront data requests that, in their national legal system, are potentially illegal.[17] This establishes a two-layer scenario of a system where global northern institutions have clarity under the law and enforceable rights, and pressuring Global South jurisdictions into compliance without any legal response in kind.[18] Such asymmetries are not merely technical oversights but flaws within the system that displaces actors within lower-capacity legal systems, in the form of athletes, into a subordinate position to those international regulators. To handle the same, anti-doping governance should adopt a base to come up with interoperable data-sharing frameworks based on international human rights law instead of the alleged interchangeability of jurisdictions, with the articulation of the jurisdictional boundary and enforceable protections for the interested athletes.

The whereabouts stipulation is the key aspect of the out-of-competition testing program of WADA, and it is representative of the escalation of surveillance in anti-doping governance. Those in the registered testing pool are expected to submit daily information, making it known where they are, at what time, and within what time frame they should be available to be tested at any moment.[19] Missing three tests or failing to provide the correct whereabouts in 12 months may result in a ban that is equivalent to a positive drug analysis.[20] Although the policy is aimed at increasing the integrity of testing, it has a very invasive price, forcing athletes to always be under constant monitoring of their private lives.[21] Critics argue that such a degree of control that lacks meaningful consent or

16 Oskar MacGregor, *Anti-Doping, Whereabouts, and Privacy: An Ethico-Legal Analysis of WADA's Whereabouts Requirements* (Swansea University (United Kingdom) 2013) <https://search.proquest.com/openview/bf36bb9d7781e34bd08640b94f3a0862/1?pq-origsite=gscholar&cbl=2026366> accessed 21 July 2025.

17 Daniel Read and others, 'The Challenges of Harmonising Anti-Doping Policy Implementation' (2024) 27 Sport Management Review 365

18 Amichai Cohen and Yuval Shany, 'Beyond the Grave Breaches Regime: The Duty to Investigate Alleged Violations of International Law Governing Armed Conflicts' (2011) 14 Yearbook of International Humanitarian Law 37

19 WADA (n 4)

20 MacGregor (n 16)

21 Julia Ellen Cook and others, 'The Ethics of Sports Integrity Investigations and the Power of Sport Integrity Bodies to Compulsorily Demand Information and Personal Devices from Athletes' [2025] International Journal of Sport Policy and Politics 1

recourse thus undermines autonomy and disproportionately affects athletes without institutional support or legal literacy.[22] In other parts of the world where data protection laws are not well established, the measure threatens to undermine the internationally established right to privacy without providing any similar protection under laws or ethics.

The Athlete Biological Passport (ABP) is an ongoing change in the paradigm of detection-based anti-doping towards a longitudinal anti-doping surveillance.[23] Currently applied by WADA since 2009, the ABP measures a combination of individual biomarkers, i.e., the levels of hemoglobin or steroidal profiles, continuously, to detect any deviations signaling the athlete is using doping.[24] In contrast to off-drug tests, ABP data is collected over time, retained for as much as ten years, and it can be used to initiate targeted testing or sanction proceedings, often without direct evidence of the presence of a prohibited substance.[25] Although such an approach improves the ability to detect targets, it raises major issues related to data retention, proportionality, and informed consent. Athletes, specifically those from the Global South, may be unaware of the manner in which their biological data is utilized, shared, or challenged in legal proceedings.[26] These risks are made worse by the lack of consistency of legal protection between jurisdictions: long-term biometric surveillance can proceed with minimal scrutiny or remedy and may interfere with core rights to privacy and control over data as a result.

One of the scarcely investigated and yet growing aspects of anti-doping oversight is the utilization of algorithm systems and artificial intelligence (AI) in targeting choices, and specifically in relation to ABP analytics and danger-profiling software.[27] The seemingly constant accumulation of training, performance, biometric curves, and more also allows WADA and other affiliated

22 Francisco Javier Lopez Frias and Mike McNamee, 'Autonomy, Relationality, and Brain-Injured Athletes: A Critical Examination of the Concussion in Sport Group's Consensus Statements between 2001 and 2023' (2024) 18 Sport, Ethics and Philosophy 383

23 Tiia Kuuranne, Martial Saugy and Norbert Baume, 'Confounding Factors and Genetic Polymorphism in the Evaluation of Individual Steroid Profiling' (2014) 48 British journal of sports medicine 848

24 Yaoyao Wang, 'Biomarker, Metabolomics and Doping: A Novel Approach to Detect Drug Misuse' (PhD Thesis, King's College London 2017) <https://kclpure.kcl.ac.uk/portal/files/73349316/2017_Wang_Yaoyao_1223760_ethesis.pdf> accessed 30 July 2025

25 Millán Aguilar and others, 'Thirteen Years of the Fight against Doping in Figures' (2017) 9 Drug Testing and Analysis 866

26 Prof Ghorbani Asiabar, Morteza Ghorbani Asiabar and Alireza Ghorbani Asiabar, 'A Comparative Study of Legal Challenges in the Ownership of Biometric and Performance Data of Athletes at the International Level' [2025] ScienceOpen Preprints <https://www.scienceopen.com/hosted-document?doi=10.14293/PR2199.001715.v1> accessed 30 July 2025

27 Dragčević, Pandžić Jakšić and Jakšić (n 4)

organizations to increasingly exploit models of various predictive capabilities towards prioritizing athletes at random to test.[28] However, these algorithms are not impartial; they are essentially programs that contain the assumptions, priorities, and blind spots of the people who built them.[29] All systems receive data that is often based in the Global North and might be calibrated to detect people who train at altitude or have diet regimes or underreport injuries, which are not actually suspicious but may be an anomaly to the statistical data.[30] In addition to that, the proprietary nature of these tools has led to a lack of transparency by both the NADOs and the athletes regarding the manner in which the testing targets are created, bringing into question due process and responsibility.[31] Such systems are vulnerable to becoming repeat performances of structured bias because of a lack of accountability in the form of an algorithmic audit or failed redress by athletes. It will be necessary to infuse a sense of fairness and explainability into the AI-based anti-doping procedures, so that the introduction of digital profiling that would excessively burden already-marginalized athletes should be avoided.

Randomized testing, centralization of data storage, and data sharing across national boundaries are the main pillars of anti-doping systems.[32] Such measures as random testing can be justified because they attempt to make it unpredictable when an athlete might use a performance-enhancing drug, which is an exploitable weakness.[33] Competitors in the registered testing pool can be chosen to give samples at any stage, on the basis of statistical models, biological profiling or from performance patterns (WADA, 2021).[34] The resulting data, including urine and blood samples, geolocation records, and medical confessions, are stored in such centralized systems as the Anti-Doping Administration and Management System (ADAMS).[35] Under the International Standard of WADA on Protecting privacy and personal information (ISPPPI),

28 Hyunji Ryoo and others, 'Identification of Doping Suspicions through Artificial Intelligence-Powered Analysis on Athlete's Performance Passport in Female Weightlifting' (2024) 15 Frontiers in Physiology 1344340

29 Bruno Lepri and others, 'Fair, Transparent, and Accountable Algorithmic Decision-Making Processes: The Premise, the Proposed Solutions, and the Open Challenges' (2018) 31 Philosophy & Technology 611

30 Nicholas Hailey, 'A False Start in the Race against Doping in Sport: Concerns with Cycling's Biological Passport' [2011] Duke law journal 393

31 Shaun Star and Sarah Kelly, 'A Level Playing Field in Anti-Doping Disputes? The Need to Scrutinize Procedural Fairness at First Instance Hearings' (2021) 21 The International Sports Law Journal 94

32 Karla Hemming and others, 'Ethical Implications of Excessive Cluster Sizes in Cluster Randomised Trials' (2018) 27 BMJ Quality & Safety 664

33 Ryoo and others (n 28)

34 WADA (n 4)

35 MacGregor (n 16)

these datasets can be accessed or transferred between the recognized bodies, such as national anti-doping organizations (NADOs), accredited labs, and Global sporting federations.[36] But there are no harmonized legal frameworks in this international exchange of sensitive data, which causes issues of data sovereignty, oversight, and data security that can be vulnerable even to the lowest standards of protection at the domestic level of the sports organization of the athlete.

The globally integrated data environment has evolved into what critics describe as a "surveillance architecture" embedded within the anti-doping regime.[37] By offering permanent geolocation tracking, prolonged monitoring of biomarkers, and unlimited data retention, the system provides an unparalleled depth of scrutiny on the bodies and actions of athletes. Even though justification involves protecting clean sport, the health of athletes, and maintaining the general faith of the population, the strategies employed in accomplishing the objectives commonly extend to the area of disproportionality, especially when the athletes are deprived of the legal instruments to challenge or oppose the data activities themselves. The limits between what constitutes legal regulation and overreach are becoming more and more difficult to detect without obvious international protection. This burden is increased in the athletes of the Global South due to an inadequate legal framework, poor institutional assistance, and insufficient informed consent mechanisms. In such a way, the system of fairness, on the one hand, threatens to institutionalize the inequality to be institutionalized, and, on the other hand, to violate the fundamental rights.

3.0 International Human Rights and Digital Privacy Norms

The right of privacy is a basic human right, which is reflected in several international legal instruments, as Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention on Human Rights (ECHR).[38] These clauses assure security against unwarranted or illegal encroachment into one's privacy, home, or correspondence. Although they are not absolute rights, they can be subjected to limitations in the name of preservation of the order or health of the populace, so long as the limitations satisfy the criteria of legality, necessity, and proportionality. Regarding anti-doping regulation and especially the use of such technological tools as the whereabouts system and biological passports, athletes are constantly monitored

36 ibid
37 Pinto (n 10)
38 Kristian P Humble, 'Human Rights, International Law and the Right to Privacy' (2020) 23 Journal of Internet Law 1

and their data is extracted, with no suspicion being needed on an individual level.[39] This raises concerns about whether the extent and intrusiveness of such practices can be justified under international human rights norms. Regarding athletes in the Global South, who might lack judicial protection, as it may be insufficient or underdeveloped, the likelihood of them being abused is higher, whereas the chance to pursue the violation of privacy through a judicial path is minimal. As a result, although the purpose of anti-doping systems is legitimate in regulatory terms, their use does not always pass the standards of allowable intrusions under the international law of human rights.

Data Protection is a human right that was long neglected in the international human rights discourse but that has gained a life of its own in the digital era.[40] The General Data Protection Regulation (GDPR) of the European Union has established a standard that is valued globally, by giving individuals the rights to find out, change, and delete their data, to be informed about the use of their information, and to object to illegal data processing.[41] Similarly, the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) introduces regional data protection and data controller responsibility standards.[42] Such frameworks are, however, unevenly adopted, and numerous countries in the Global South do not have any enforceable data protection law or sufficient enforcement practices.[43] Lack of such protection is especially dangerous in anti-doping, where, based on no consent and with no legal avenues, an athlete's sensitive data, such as biometric and geolocation data, can be stored, transferred or analyzed without them having any control over the process. Besides, the centralized data-sharing infrastructure of WADA does not always align well with these emerging norms, especially given its extraterritorial operations. The combination of the fact-value asymmetry existing between the global surveillance patterns practiced by WADA and the legal and regulatory regimes that protect the rights of sportspeople in different jurisdictions constitutes a clear normative weakness. The exposure of athletes in the low- and middle-income countries to the risk of violations of their rights is disproportionately high.

39 Pinto (n 10)

40 Stefan Loubichi, 'General Data Protection Regulation (GDPR) of the European Union. What Had to Be Considered until 25 May 2018' <https://inis.iaea.org/records/45gtd-dnb81> accessed 30 July 2025

41 ibid

42 African Union, 'African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)' [2014] Addis Ababa: African Union

43 ibid

Closely linked to the right to privacy and data protection is the right to informed consent and freedom from coercion. These considerations are core bioethics and international law, especially through such declarations as the Declaration of Helsinki and the UNESCO Universal Declaration on Bioethics and Human Rights.[44] When seeking informed consent, it must be ensured that the people are aware of the nature, scope and implications of the data that is being collected from them, and they would be in a position to accept or not be in the position of collection of the data without any penalty.[45] In the anti-doping environment, consent is, nonetheless, in many cases, presented as a prerequisite to eligibility to compete, so that it would be characterized as non-voluntary. Those athletes who cannot afford legal counsel or are digitally illiterate cannot be fully aware of what happens to their biological and location data, how they are used, stored, and shared in various jurisdictions.[46] This forced agreement is particularly threatening to the Global South athletes, as the educational, language, and infrastructure factors equally contribute to undermining the actual consent.[47] The very restraint of anti-doping constructed in the current international system turns what ought to be a rights-based agreement into a matter of participation, violates the ethical principles of informed consent, and generates severe doubts regarding principles of fairness, transparency, and autonomy in global sports.

One of the areas where the world bureaucracy of anti-doping is lacking is in procedural protections, particularly for athletes in the Global South who may be enforced without the benefit of better and fuller judicial protections.[48] Cases proceeding based on WADA inquiries are usually resolved through a private arbitration institution, the Court of Arbitration for Sport (CAS), which is based in Lausanne, Switzerland. [49] Despite its common use in international sport, CAS does not share numerous features of the judicial systems that are available to ordinary citizens, not to mention hearings being open, state control, or exercising the right to appeal to national courts.[50] Among the advantages of the inaccessible judicial system, on top of limited financial resources and language barriers, there are particularities of the legal procedures that might

44 Roberto Andorno, 'Global Bioethics at UNESCO: In Defence of the Universal Declaration on Bioethics and Human Rights' (2007) 33 Journal of medical ethics 150

45 Kimberly Kessler Ferzan, 'Consent and Coercion' (2018) 50 Ariz. St. LJ 951

46 Star and Kelly (n 31)

47 ibid

48 ibid

49 Tribunal Arbitral du Sport, 'Court of Arbitration for Sport' [2024] URL: https://www. tas-cas. org/en/index. html (25.09. 2020 p.) <https://www.wada-ama.org/sites/default/files/resources/files/cas_2008_a_1564_busch.pdf> accessed 30 July 2025

50 Duval (n 8)

become torturous to athletes who do not have legal representation or have little understanding of the legal procedure.[51] International law scholars have voiced alarm that the privatized system could weaken the provisions of Article 14 of the ICCPR that stipulate a right to a fair and public hearing before a tribunal of appropriate competence that is impartial.[52] This is because privatizing justice in anti-doping not only narrows substantive rights but can also lead to the institutionalization of inequalities in the sense that only the more-resourced will have access to the international arena in which they can access redress. This unequally puts players representing low-resource jurisdictions unable to access a legal infrastructure or be represented.

The current global anti-doping regime, as it exists, tends to work in a way that largely trumps or overwhelms the existing human rights provisions, especially in situations where the legal frameworks prove to be undeveloped or applied in a spotty fashion. The intrusive nature of surveillance by WADA using the centralized administration, e.g., ADAMS and the Athlete Biomedical Passport, seldom reflects jurisdictional differences in privacy and data protection legislation.[53] The General Data Protection Regulation (GDPR) of the European Union is a broad and legally binding standard that requires the minimization of data, limiting its use, and mandates the existence of strong consent measures, and gives individuals enforceable rights to dispute unlawful data processing.[54] On the one hand, sub-Saharan Africa, South Asia, and Latin America mostly do not have such legal tools or, at best, very young data protection legislation, much of which is not enforced.[55] This disparity leads to the de facto stratification of the rights of athletes, with those participating in Global North events enjoying high levels of legal protection and those in Global South facing increased levels of vulnerability. This inequality is worsened by the indiscriminate enforcement of WADA procedures, which are applied without consideration of local legal requirements, and that threatens to institutionalize a dual system of privacy and consent. Such tension raises the question of the sensitivity of the present anti-doping governance to international legal requirements and the necessity of more balanced, less neutral regulation.

The extraterritorial application of anti-doping surveillance services creates a

51 Moni Wekesa, 'Regulation of Doping in Sports: Implications for Kenya' (PhD Thesis, University of Nairobi, Kenya 2010) <https://erepository.uonbi.ac.ke/handle/11295/4897> accessed 19 June 2025

52 Benedict Kingsbury, 'The Concept of 'Law'in Global Administrative Law' (2009) 20 European Journal of International Law 23

53 Pinto (n 10)

54 MacGregor (n 16)

55 Wekesa (n 51)

paradox in the law: WADA has binding demands everywhere on the globe, but it is seldom answerable to domestic or global law. It usually ignores constitutional privacy safeguards and cannot be called into question by national human rights authorities or international courts, like the African Court on Human and Peoples Rights or the Inter-American Commission on Human Rights (Greenleaf & Cottier, 2020).[56] Things are made more complicated by the legal fiction of voluntary participation by athlete consent, to which the WADA surveillance infrastructure, particularly by ADAMS and the ABP, falls outside the legal jurisdiction of the majority of jurisdictions in the Global South.[57] It has been claimed that this is a type of unilateralism as the norms are exported without any means of reciprocated oversight or redress.[58] Such a vacuum is further aggravated by the fact that there are no binding treaties or intergovernmental agreements, which could bring WADA into the domain of international legal regulations in the form of digital operations. With no legal requirement to honor local privacy regulations or be subjected to rights-based review processes, WADA acts as an exception to the rule of international norms, which it has no legal responsibility to answer to, despite its claims of universality. Closing this gap is the only way to avoid recreating an institution in which the data governance exists in its accelerated frenzy, where it is no longer connected to the rights it purports to defend.

4.0 Disproportionate Burdens on the Global South

As demonstrated by numerous studies, enforcing anti-doping unjustly affects the athletes of the Global South, who are frequently punished without sufficient representation, protection measures, or awareness of their digital rights.[59] In Kenya, in particular, several athletes have faced sanctions imposed by the Anti-Doping Agency of Kenya (ADAK) on what have been claimed as violations related to missed whereabouts submissions or by way of positive tests of contaminated supplements, usually without obtaining adequate legal services or expert scientific assistance.[60] Likewise, confusion regarding the testing process and the absence of informed consent have been reported

56 Yohannes Eneyew Ayalew, 'Untrodden Paths towards the Right to Privacy in the Digital Era under African Human Rights Law' (2022) 12 International Data Privacy Law 16

57 MacGregor (n 16)

58 Kathryn Henne, 'WADA, the Promises of Law and the Landscapes of Antidoping Regulation' (2010) 33 PoLAR: Political and Legal Anthropology Review 306

59 Yohannes Eneyew Ayalew, 'Untrodden Paths towards the Right to Privacy in the Digital Era under African Human Rights Law' (2022) 12 International Data Privacy Law 16

60 Byron Omwando Juma, 'Kenyan Athletes' Experiences with Anti-Doping Rule Violations' (PhD Thesis, University of Illinois at Urbana-Champaign 2024) <https://www.ideals.illinois.edu/items/134232> accessed 19 June 2025; Wekesa (n 51)

among the athletes residing in Nigeria and India, especially athletes with a rural training background.[61] Jamaican athletes have also spoken up against the inconsistencies in the disciplinary proceedings and inadequate education about their rights governed by the international anti-doping systems.[62] These examples highlight structural imbalance in the infrastructure of law systems and judicial review, as well as the fact that athletes in resource-scarce environments are less empowered to dispute procedural anomalies or demand protection of their privacy. The created landscape of enforcement not only shows a regulatory vacuum but also a more profound structural inequality built into the governance of sport globally.

Coerced compliance is a defining, yet underexamined, characteristic of global anti-doping enforcement, specifically among athletes from the Global South who often lack the necessary legal and digital literacy to allow them to navigate the complex regulatory systems.[63] The formal conditions of agreement to anti-doping procedures do mandate the consent of athletes to the collection of data; however, since the system is practically universal, the effect of such a requirement is a conditional involuntariness of athlete data collection.[64] A lot of athletes leave their signature on consent forms or address whereabouts without being aware of the reasons why this would affect their privacy, data storage, or international data transfer. The athletes are particularly vulnerable to procedural exploitation in situations where there are weak education systems and low anti-doping literacy levels, namely, in rural training environments in Kenya, India, or Nigeria.[65] This imbalance is also supported by imbalanced power relations between athletes and the sporting authorities, where failure to cooperate, despite or notwithstanding, may lead to penalties and fines that are similar to those that are meted out in a doping violation. This process turns the aspect of regulatory compliance into a state of being coerced to participate and this act negates the aspects of ethical premises of consent and poses crucial concerns in the international norms of human rights with regard to autonomy, informed consent, and avoidance of exploitative institutional preferences.

61 Macellina Y Ijadunola and others, 'Perception of Nigeria University Athletes about Performance-Enhancing Substances and Drug Testing' (2018) 10 International Journal of Sport Policy and Politics 567

62 SC Turfus and others, 'Supplementation Practices, Perceptions and Knowledge about Anti-Doping among Jamaican High School Athletes' (2019) 7 Performance Enhancement & Health 100145

63 David Orozco, 'A Systems Theory of Compliance Law' (2019) 22 U. Pa. J. Bus. L. 244

64 Rachel Thompson, 'Ethical and Governance Challenges in Population Biobanking: The Case of the Global Anti-Doping Administration & Management System' <https://cronfa.swan.ac.uk/Record/cronfa61187> accessed 30 July 2025

65 Juma (n 60)

Global anti-doping governance architecture is largely established by the institutions based in the Global North, i.e., World Anti-Doping Agency (WADA), International Testing Agency (ITA), and the European and North American-based national anti-doping organizations. These institutions bring normative and operational controls of these compliance mechanisms, but they usually lack sensitivity towards regional differences in legal capacity, cultural context, or infrastructural preparedness.[66] Global South athletes unfairly receive punitive action in case of technical and procedural violations, such as failure to file, therapeutic use exemption (TUE) mistake or language barrier during testing procedures, unlike their Global North peers who have access to similar means of legal protection, or an organization of protection.[67] This inequality constitutes an institutional inequity that strengthens the geopolitical structures within the sport, whereby its Global North representatives not only frame the rules, but they also control the adherence to the rules. Moreover, the selective enforcement method and unreliable sanctioning trends present a concern about unfair implementation, which adds to the image of regulatory colonialism of anti-doping policies.[68] The outcome is an enforcement regime that, although supposedly universal and neutral, tends to recreate global inequalities and render anti-doping a largely illegitimate regime of alleged equity.

Inequality in the application of anti-doping systems in the world is highlighted when issues of intersectionality, like gender, ethnicity, and socioeconomic status, are ignored in policy formulation and enforcement. The Global South athletes tend to have systemic disadvantages, such as the lack of access to legal representation, procedural comprehensibility, and anti-doping training.[69] In this setting, women are the most susceptible ones. Their vulnerability to punitive ramifications is compounded by obstacles, including constrained access to the digital infrastructure, diminished education levels, and underrepresentation in national and international sports governing bodies.[70] Research establishes that women in sports in areas such as East Africa or South Asia will regularly suffer from chronic underfunding and organizational neglect, especially in disciplines that are not well-resourced, such as women's football.[71] This places

66 Barrie Houlihan and Borja García, 'The Use of Legislation in Relation to Controlling the Production, Movement, Importation, Distribution and Supply of Performance-Enhancing Drugs in Sport (PEDS)' <http://pstorage-loughborough-53465.s3.amazonaws.com/17257718/UNESCOLegislativeResearchReportFINAL.pdf> accessed 30 July 2025

67 Star and Kelly (n 31)

68 Faraz Shahlaei, 'State-Sponsored Doping and International State Responsibility: Caveats of the International Anti-Doping System' (2023) 51 Syracuse J. Int'l L. & Com. 237

69 Star and Kelly (n 31)

70 Juma (n 60)

71 Martha Saavedra, 'Football Feminine – Development of the African Game: Senegal, Nigeria and

them in a predicament of being more vulnerable to procedural breaches such as inefficiencies in therapeutic use exemption (TUE) filing or misunderstandings in test processes.[72] The ethical neutrality of global anti-doping programs raises concerns about the justice of anti-doping programs under these intersectional inequalities, particularly when investigating them within different cultural and infrastructural settings. Regulatory frameworks are needed that take into consideration not only geographic disparities, but also the cumulative burdens that exist due to the marginalization of Global South athletes who face multiple barriers.

A structural disadvantage like language restriction, digital illiteracy, and technology access disparity further excludes Global South athletes in the mechanism of anti-doping. Compliance with systems such as ADAMS and the athlete biological passport requires regular digital interaction, proper data input, and regular access to the internet, all of which are not consistent with the actual realities in the environment of low-resource countries.[73] Due to little fluency in English and French, many athletes have to provide information about their whereabouts in these languages and end up with miscommunication and errors in procedure that may lead to sanctions.[74] In addition, the difficulty with user interfaces the lack of culturally-adjusted digital training lead to exclusion, especially among those athletes who have not been trained before in the digital world. Many sportspeople in Africa, South Asia, and the Caribbean reside in underserved regions or rural areas, where regular access to the internet, which is a requirement of real-time compliance and testing organizations, is not available.[75] Such technological and linguistic gaps cannot be reduced to logistical ones; those are structural inequalities that compromise the legitimacy and fairness of anti-doping enforcement. Failure to tolerate such differences goes against the premise of substantive equality and raises concern over the international homogeneity proclaimed by the anti-doping regimes.

The current frameworks of both literature and regulatory focus regarding the implementation of various anti-doping measures in the Global South tend to focus on a handful of what can be conceptualized as the high profile nations;

South Africa' (2003) 4 Soccer & Society 225

72 Timothy Kipkemboi Sang, 'Doping in Athletics A Critical Analysis on the Right to a Fair Hearing of an Accused Athlete' <https://su-plus.strathmore.edu/bitstreams/f6690627-a942-45f1-a68e-5cddabb0f3f6/download> accessed 21 July 2025

73 Houlihan and García (n 63)

74 Read and others (n 17)

75 Nir Kshetri, 'The Economics of the Internet of Things in the Global South' (2017) 38 Third World Quarterly 311.

Kenya, Nigeria, and Jamaica, which overshadows the actual reality of these massive areas, including Pakistan, Bangladesh, Indonesia, or Colombia, in terms of how both the athletes and administrative bodies manage to cope with this specific issue within their contexts. According to reports by the South Asian and Latin American federations, athletes in these areas do not always understand what accredited facilities are, cannot timely translate procedures with translations of declarations, and do not have a stable system of therapeutic use exemptions (TUE).[76] In most instances, there are no education campaigns or proper communication of the rights of an athlete under the World Anti-Doping Code before testing. Furthermore, the narrative might also be effective symbolically because the international authorities often engage with apparently exerting pressure to be perceived as vigilant, even in situations where the negligence at the level of the Global North is not subject to equal pursuit.[77] This is selective publicity that perpetuates a regulatory contradiction that derails the validity of anti-doping initiatives. The widening of the observed scope of a few case studies demonstrates an entirely larger structure of institutional abandonment and unequal enforcement that has since remained elusive to substantive redress.

5.0 Ethical Dilemmas: Balancing Anti-Doping Goals with Human Rights

The anti-doping system in the world exists in a built-in ethical dilemma between the need to preserve the integrity of sport and the health of the athlete on the one hand, and the need to respect the personal rights to privacy, autonomy, and informed decision-making on the other. The world's Anti-Doping code preaches the idea of a spirit of sport based on fairness, health, and excellence values.[78] Nevertheless, such purposes have required invasive monitoring systems, such as compulsory biological surveillance, tracking by geolocation, and extensive data retention, which fall under the rights bound by the international system of human rights. The right to privacy is recognized in the International Covenant on Civil and Political Rights (Article 17) and the European Convention on Human Rights (Article 8), a presumption that the state or other institutions may not intrude upon that right without reasonable justification and proportionality.[79] Whereas anti-doping is aimed at creating

76 Read and others (n 17)

77 L Patterson and H Staff, 'Understanding and Influencing Global Coach Anti-Doping Education through the Development of an International Framework' <http://eprints.leedsbeckett.ac.uk/id/eprint/7517/7/UnderstandingAndInfluencingGlobalCoachAntiDopingEducation-PATTERSON.pdf> accessed 21 July 2025

78 WADA (n 4)

79 Özgür H Çinar, 'The Right to Privacy in International Human Rights Law' (2019) 13 Journal of Information Systems & Operations Management 33

a level playing field, the methods that the body employs undermine athletes' bodily autonomy and informed consent, particularly when participating in the data collection process is framed as a non-negotiable precondition for eligibility to compete; therefore, it may be difficult to distinguish between consent and coercion in the anti-doping agenda.

Due to the comprehensive nature of surveillance done by the anti-doping regimes, in particular, the whereabouts clause that requires athletes to have their location monitored 24/7, there are compelling ethical issues of necessity and proportionality. The Registered Testing Pool (RTP) athletes are compelled to declare their whereabouts to the positioning authority within one hour each day throughout the year, usually with an unknown rationale based on rational suspicion.[80] This 24/7 surveillance resembles the one traditionally deployed at the level of states in cases of high-risk individuals, not to mention citizens who are assumed to be innocent. Ethically data-wise, all these measures are justifiable only to the extent to which they comply with quantities of necessity (i.e., the least amount of force that could be used) and proportionality (i.e., the damage prevents a bigger one than the right violated).[81] Such critics assert that the general, untargeted character of these requirements cannot satisfy these standards and that it is particularly inapplicable when these are imposed consistently across countries with significant differences in the level of digital infrastructure and of protections on their rights.[82] The lack of solid, personalized risk detection systems calls into question the argument that contemporary anti-doping surveillance does not infringe on ethical standards and furthers the necessity of rights-based, proportionality-based reforms.

Bioethics and data ethics principles put the current perception of anti-doping systems that athletic integrity is of importance to citizens and that the interests of the state justify the wide-reaching and unconstrained actions on the lives of athletes into question. Although it is good that we want to protect fair play and the health of the athlete, they must be put in balance with the right of an individual to bodily autonomy, informed consent, and digital dignity. [83]

80 Marjolaine Viret, 'Legal Constraints on Evidence in Anti-Doping' in Marjolaine Viret, *Evidence in Anti-Doping at the Intersection of Science & Law* (TMC Asser Press 2016) <https://link.springer.com/10.1007/978-94-6265-084-8_3> accessed 30 June 2025

81 Shuang Lu Frost, *Moralizing Disruption: China's Ride-Hailing Revolution* (Harvard University 2019) <https://search.proquest.com/openview/5658f223b1e235f0bb20f6eb1d80095e/1?pq-origsite=gscholar&cbl=18750&diss=y> accessed 30 July 2025

82 Mike J McNamee and Lauri Tarasti, 'Juridical and Ethical Peculiarities in Doping Policy' (2010) 36 Journal of Medical Ethics 165

83 James F Childress and Tom L Beauchamp, 'Common Morality Principles in Biomedical Ethics: Responses to Critics' (2022) 31 Cambridge Quarterly of Healthcare Ethics 164

Such an approach to anti-doping infringes a fundamental ethics principle of informed consent, which, in turn, is violated by the fact that, in anti-doping regimes, participation in the program is de facto compulsory, and any refusal has the same outcome as a positive test.[84] Further, the idea of digital dignity, as the right to manage one's data in the digital world, is not usually considered in the design or regulation of anti-doping technologies.[85] This moral flaw reveals the necessity of governance frameworks that account for individual agency and, at the same time, effective control, especially over those athletes whose jurisdiction is weaker in protecting them legally and who are less informed about digital rights.

Anti-doping systems are becoming more paternalistic, where they assume that there is a necessity to monitor athletes (especially those in the Global South) and regard them as more prone to unethical conduct or more prone to manipulation. This position usually takes the form of what people refer to as soft coercion, where the consent seems official when, in fact, it has no repercussions as a result of structural necessities and the unavailability of other options.[86] Low-resource athletes are overrepresented among those who are subject to invasive monitoring, but not to any of the required safeguards, an example of unequal global power in the regulatory regime.[87] This might have been associated with an ethical excess where the authorities had deemed it necessary to exercise excessive control on the basis of upholding the integrity of the sport without regard to the autonomy and agency of the people. Such asymmetric inspection props up postcolonialism structures in the international governance of sport, wherein it views the Global South athletes not as equal team players but as students in need of rediscipliningby an outside source. The paternalism proved that, in the absence of contextualized safety nets, it has the potential to trample over rights in the name of morals and equity.

The critical moral defect of the existing anti-doping regime is that it is based on the model of a single approach to the problem without adjusting to the legal, infrastructural, and cultural peculiarities of different states. The standards harmonized worldwide and set by WADA are universal, and they

84 Roger Pielke and Erik Boye, 'Scientific Integrity and Anti-Doping Regulation' (2019) 11 International Journal of Sport Policy and Politics 295

85 Siva Vaidhyanathan and Chris Bulock, 'Knowledge and Dignity in the Era of "Big Data"' (2014) 66 The Serials Librarian 49

86 Kimberly Kessler Ferzan, 'Consent and Coercion' (2018) 50 Ariz. St. LJ 951

87 Education Partnerships, 'Virtual Mentor American Medical Association Journal of Ethics March 2010, Volume 12, Number 3: 143-252. Global Health Ethics in Practice' (2010) 12 Global Health 143

do not provide much room for single jurisdiction rights or socioeconomic weaknesses.[88] Famous athletes in the Global North usually have efficient national judicial institutions, privacy laws (e.g., GDPR), and professional networks to support them, whereas their Global South counterparts have to operate in a black box with no procedural protection, as they lack means of redress.[89] Lack of differentiated levels of protection of data, the practice of informed consent, and the mechanisms of appeals enshrines international disparities in the name of impartiality. This institutional nonchalance to legal pluralism not only invalidates the legitimacy of anti-doping governance, but at the same time, it creates great concerns in terms of justice and due process. Considering and acting on the root cause of the uneven topography of legal capacity across the globe is part and parcel of a genuine system of equity, as opposed to a legal universalism that favors the resourced.

6.0 Towards Equity: Recommendations and Reform Pathways

6.01 Procedural Reforms

The development of the procedural requirements to decrease justice gaps installed in the existing anti-doping practice must focus on context-sensitive protections, being conscious of the legal rights and self-regulation of athletes. One of the main suggestions is the adoption of the mechanism of informed consent that reflects the social-legal reality of different jurisdictions. This comes along with not only serving the consent documents in the native languages of the athletes but also making sure that they understand by encompassing the necessary explanations in a culturally acceptable manner and using the assistance of a legal aid in case there is a need.[90] Also, information collection and disclosure should be dictated by the concepts of necessity, proportionality, and legality, according to the international standards of data ethics and human rights.[91] A potentially more serious privacy concern is the long-term retention of biometric and whereabouts data, where this is decoupled from active investigations, which in less regulated settings are not usually challenged. The extent and the number of days that data is, in fact, collected should also be reduced unless justifiably indicated to reset how the competing

88 Viret (n 80)

89 Star and Kelly (n 31)

90 Arja Halkoaho and others, 'Cultural Aspects Related to Informed Consent in Health Research: A Systematic Review' (2016) 23 Nursing Ethics 698

91 Luciano Floridi and Mariarosaria Taddeo, 'What Is Data Ethics?' (2016) 374 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20160360

priorities between the anti-doping agenda and the overarching rights measures play out, opening the pathway to a more balanced and rights-respecting enforcement practice.

In order to make procedural reforms not just aspirational, deployment of such reforms must be pegged upon mechanisms, which are not only enforceable but also adapted to local realities. Practically, the lack of culturally and legally considerate protocols results in blanket implementation, which dismisses any difference between the digitalized space, education and institutional infrastructure. As an example, rural athletes in developing nations, such as Uganda or Bangladesh, can enter anti-doping Enforcement restrictions without knowing what they have done, because in different forms of modern technologies, they have not had such previous experiences.[92] As a solution to meet such procedural injustice, it is proposed that the reform goals should involve compulsory instruction of rights to the athletes, localized data privacy instruction and pre-consent counseling handled by reputable intermediaries or the athletes' support staff. Moreover, national-level structural implementation of independent ombudspersons of athletes would be an addition to the layer of responsibility and equity because they would be tasked with supervision of the process of informed consent and would be able to step in whenever a process is not clearly described. These options highlight that procedural reform should not only focus on ethical motive, but the legal design and technological backing too and without which the Global South athletes will not be able to access the sophisticated data regimes of anti-doping enforcement in a permanent disadvantage.

6.02 Legal Safeguards

Other than procedural changes, legal protection should be enacted to respond to the increasing scope of anti-doping monitoring effectively. Most of the countries in the Global South do not have stringent domestic data protection laws that protect athletes subjected to data practices, leaving a vacuum in terms of regulations.[93] That disparity requires immediate regional convergence, including the effective enforcement of the African Union Convention on Cybersecurity and Personal Data Protection (AUCC) or a similar regional initiative in Asia and Latin America. At the same time, a WADA Charter of Digital

92 Read and others (n 17)

93 Pinto (n 10)

Rights is a globally binding instrument that could provide a minimum of rights to athletes (data transparency, its correction or erasure, access to legal redress). A charter of this sort would reflect the rationale of the European Union General Data Protection Regulation (GDPR), but it would also reflect the peculiar weaknesses of the athletic environment. Those protections would also instill legitimacy, fairness, and adherence to emerging global standards on digital rights entrenched within the WADA institution.

The lack of legally enforceable protection has already caused real injuries, such as the mishandling of athlete data that cannot be recouped, or cases where penalties have been issued on seemingly shoddy procedural grounds and cannot be appealed in court. In an environment of the absence of digital jurisdiction, or courts being affected by those of sports, athletes can even be left outside the justice system. To be viable in terms of operations, legal reforms should be more than a list of protections and adopt a Charter of Digital Rights that specifies obligations enforceable by WADA, such as independent oversight groups, transparency audits, and complaint channels, depending on jurisdiction. Examples of precedents in the international treaty systems, which include the Convention 108+ on data protection entered into the Council of Europe, show that their enforcement relies on compliance checks conducted regularly and multi-stakeholder governance.[94] Regional institutions like the African Court on Human and Peoples Rights or the RED GEALC in Latin America would have a monitoring role to play, provided they are given the power. In this regard, legal protections should not be carried out in the form of rhetoric statements but precisely entrenched in the sort of systems that can enable players, particularly those who belong to jurisdictions that are underrepresented, to exercise their rights in a form that is practical and accessible to them.

6.03 Support Mechanisms

It is crucial to enhance the support systems so that athletes in low-resource environments are not disproportionately affected by the global anti-doping system. In the African continent, South Asia, and the Caribbean, various athletes also receive sanctions without

94 Lorna Gillies and others, 'Cross-Border Enforcement of Consumer Law: Looking to the Future.' <https://discovery.dundee.ac.uk/files/136814347/ccpb_WG_e-commerce_cross-Border_Riefa_en_4_.pdf> accessed 30 July 2025

being able to obtain legal assistance, translation services, or even proper knowledge of their rights according to WADA standards.[95] Deployment of a completely autonomous ombudsman process at the national or regional level of sports administrative bodies may offer valuable help to athletes struggling through the complexities of procedural regulations, particularly in situations when the data concerned or the process is unclear. Furthermore, institutional capacity within National Anti-Doping Organizations (NADOs) in the Global South has to be developed. Specific training on concepts of digital ethics, data protection regulation, and human rights, according to procedures, would also encourage equity and local responsibility. In the absence of these supports for structures, anti-doping regimes may promote systemic inequality that is incapable of improving sporting integrity around the world. Good reform has to have not just normative guidance but also be readily available and enforce support structures that empower all athletes in equal measure.

The system of supporting athletes should also take into consideration power imbalances that occur between anti-doping authorities and athletes who do not represent elite sporting organizations. Sportspeople in low-income nations go without any union representation and direct access to sports lawyers, and there are often those who need to converse with national anti-doping authorities who lack resources or are politically indebted to international sources.[96] Support systems, however, should not only be reactive (that is, responding to the violation) but also be preventive. This would involve establishing professional athlete-driven advocacy platforms, regional legal clinics with sports regulation expertise and collaborating with universities or non-governmental organizations with the aim of providing sports regulation digital rights training in a variety of languages. The services of support structures ought also to be computerized and decentralized to accommodate sportspeople in rural or seemingly conflict regions where physical infrastructures are minimal. More importantly, institutional independence and accountability are what matter to the success of these mechanisms. Support services should be safeguarded against retaliation and be given the mandate to dispute both domestic and global enforcement in instances in which procedural injustices

95 Aahna Mehrotra and Aman Gupta, 'Critical Analysis of the WADA Code 2015 with Regard to the Principles of Proportionality and Human Rights' (2017) 4 Nat'l LU Delhi Stud. LJ 101

96 Star and Kelly (n 31)

may have been committed. Without these autonomous guards against this, support structures would turn out to be rather symbolic than substantial, repeating the same inequalities, which are supposed to be defenders of equality.

6.04 Accountability

The mechanisms of accountability help to make sure that the anti-doping regimes will not be permitted to act outside the limits of legality and ethics. Regardless of the fact that WADA is open to transparency, there seems to be minimal control over mechanisms of collecting athlete data or storing and sharing the same with respect to jurisdiction.[97] The practice of independent (external) data handling audits done by other data protection agencies or sports ethics committees may help fix inherent abuses and propagate best practice within National Anti-Doping Organizations (NADOs). Moreover, they ought to grant athletes the right of recourse to an official complaint system, including an external tribunal or data protection authority, which is able to consider the complaint of inappropriate punishment or misconduct and/or maltreatment of personal information. Nowadays, the channels of appeal are frequently inaccessible, and especially those represented by low-income athletes, resulting in an absence of justice.[98] Imposing contractible accountability frameworks in anti-doping management would improve not only the credibility of the system of accountability but also the extent to which the international law norms of privacy, due process and data protection are honored, particularly recognition of vulnerable or marginalized athletes.

Accountability needs more than transparency in the process; it also needs obligations that can be enforced, independent checks and involvement of athletes in governance. The existing anti-doping system, which has been developed on the basis of soft law tools like the World Anti-Doping Code, is not binding enough to provide redress in case of a right infringement. Consequently, organizations such as WADA tend to regulate themselves without being subjected to any third-party accountability system besides the internal review or arbitration procedures that, again, are not structurally independent.[99]

97 ibid

98 Duval (n 8)

99 Stacie Gray, 'Achieving Compliance with the World Anti-Doping Code: Learning from the Implementation of Another International Agreement' (2019) 11 International Journal of Sport Policy

It is thus imperative to have a multi-level system of accountability comprising the national data protection agencies, international human rights agencies, and the athlete-led monitoring boards that have actual powers. These systems would enable affected athletes to pursue surveillance-related practices, disciplinary sanctions or mishandling of data not only in the legal framework of a sport establishment (e.g., CAS) but also in national or supra-national complaint systems. To make this work, anti-doping organizations would have to be forced to routinely report on the human rights impact assessment and subject their operations to further scrutiny by outsiders. Unless it becomes institutionalized with checks and balances in place, the prospect of an anti-doping enforcement process becoming a corrupt affair where principle operates out of sight, by default and where athletes who may need justice the most are cut out of the process, must be regarded as a real possibility.

7.0 Conclusion

Although the international anti-doping policy has its basis in the fair intention of securing clean sport, it is translated today into the system of invasive monitoring that frequently violates human rights. These types of mechanisms, including the ADAMS system, twenty-four-hour monitoring of location, and biology data storage over a long period, are, per se, interesting; however, they present serious ethical and legal issues, particularly when implemented into different socio-legal settings. As revealed in the analysis, these systems are highly disadvantaged to athletes in the Global South, who would rarely afford legal advice, data literacy, or redress mechanisms. The dominant pattern is the one-size-fits-all template that is not enough because of the differences in legal infrastructure, cultural environment and resource levels. Unless there is a significant distinction and protection, the anti-doping regime is subject to being a replica of global injustice in the shadow of fairness.

Radical changes that will reconcile the sports integrity and human dignity should be made to uphold the integrity of combating the menace of drugs in the field of sports. Researchers, policy makers, and international sporting organizations have to work collectively to make frameworks that have transparency, informed consent, and responsibilities incorporated into all stages of anti-doping administration. Harmonization of the law in the region, equitable capacity building and protections by law are crucial to the

and Politics 247

development of a setting where not only the athletes are compliant, but also empowered. Anti-doping authorities can no longer afford not to align their policies with established (internationally agreed) standards of human rights, including a right to privacy, due process, and data protection rights. The result of a rights-respecting model of anti-doping will not just enhance the ethical character of sport, but will also make certain that justice is not doled out by convenience. Against the backdrop of digital governance across the world, the sporting world needs to come out with ethical initiatives that it has created and face them with fairness, equity and respect.

In the future, policy and research innovation should shift toward bottom-up systems of enforcing the rules rather than the top-down system of establishing the rules that involve action and input by the athletes, civil populace, and the legal professional talent in all areas. It is high time that longitudinal research is done on the effects of anti-doping surveillance on human rights across different settings, especially in legal frameworks where the rule of law is not yet well-established. Also, interdisciplinary sharing of insights and disciplinary cooperation, as well as ethical expertise, can be used to develop evidence-based and ethically competent regulatory models involving technologists, ethicists, public health specialists, and legal scholars. Sporting authorities across the globe also have to invest in systems to monitor and publicize disaggregate information on the outcome of enforcement, accessibility of that appeal and systematic bias occurring within the process of testing or sanctioning. In the absence of strict oversight and encompassing transformation, the system as it stands has the risk of implementing a veneer of equity under which inequalities lurk. As the digital era further transforms the parameters of the data universe, anti-doping regulations will have to become an internationally apt and locally situated system of rules: the kind that not only embraces the intent of clean sport, but also does so in an uncompromisingly applicable manner to the dignity of any athletes, alone or in groups.

96.4% OF KENYANS CAN NOW ACCESS FASTER MOBILE INTERNET SERVICES

Through the Universal Service Fund, the Communications Authority of Kenya (CA) facilitates access to diverse communication services in every part of the country, so that no one is left behind.

For more information visit www.ca.go.ke

COMMUNICATIONS AUTHORITY OF KENYA
Opening Your World

Internet of Things (IoT) Privacy and the Law: Evaluating the Effectiveness of Kenya's Data Protection Act in a Connected Age

Njigina Macharia[1**]

Abstract

The rapid expansion of the Internet of Things (IoT) has changed modern societies by linking everyday devices into interconnected networks that produce immense amounts of real-time data. Although IoT significantly benefits sectors like healthcare, agriculture, and urban planning in Kenya, its widespread adoption raises considerable privacy and data security concerns, often without clear user consent. This article critically evaluates the effectiveness of Kenya's 2019 Data Protection Act (DPA) in protecting privacy within the IoT context. The DPA, a crucial legislative initiative shaped by the EU's General Data Protection Regulation (GDPR), defines the duties of data controllers and processors, mandates explicit user consent, and specifies breach notification protocols. However, the study indicates that the DPA encounters practical and interpretational difficulties in dealing with IoT-specific issues, such as ongoing data collection, international data transfers, and the requirement for defined security standards for IoT devices. Case studies of Kenya's smart city projects, healthcare IoT, and agricultural IoT applications reveal gaps in implementation and enforcement limitations of the Office of the Data Protection Commissioner (ODPC). A comparative examination with GDPR and South Africa's Protection of Personal Information Act (POPIA) highlights the DPA's deficiencies, especially regarding consent mechanisms, guidelines for cross-border data transfers, and institutional enforcement capabilities. The article concludes with specific recommendations, including legislative updates for ongoing consent and international data transfers, improved regulatory guidelines, bolstered ODPC resources, increased public awareness, and fostering industry cooperation. These strategies are essential for Kenya to effectively navigate technological advancements while upholding fundamental privacy rights in an increasingly interconnected environment.

Keywords: *Internet of Things (IoT), Data Protection Act (DPA), Privacy, Data Security, Data Minimisation, Cybersecurity, Healthcare IoT.*[2]

1 ** Njigina Macharia is an Advocate of the High Court of Kenya, a Certified Information Privacy Professional/Europe (CIPP/E) and the founder of Njigina Macharia Advocates. * The author acknowledges the contribution by Dr. E. O Asher's in shaping some of the arguments in this article.

2

1.0 Introduction

The exponential growth of the Internet of Things (IoT) has significantly reshaped modern societies by seamlessly integrating everyday devices into interconnected networks. IoT encompasses devices ranging from smart home appliances and wearables to sophisticated industrial sensors and autonomous vehicles, each embedded with sensors capable of generating, transmitting, and analysing vast quantities of data in real time.[3]

Globally, IoT adoption is driven by its capacity to increase efficiency, reduce costs, and enhance decision-making in healthcare, agriculture, urban planning, and industry sectors.[4] In Kenya, this technological wave is notably evident in government-backed initiatives like the innovative city projects in Nairobi and Konza Technopolis and IoT applications in precision agriculture and digital healthcare solutions.[5]

Despite their transformative advantages, the rise of IoT devices brings significant privacy and data security challenges.[6] IoT technologies depend on the ongoing collection, storage, and analysis of personal and sensitive data, often without users' explicit and informed consent.[7] As a result, IoT ecosystems have eroded conventional privacy boundaries, increasing vulnerabilities. Concerns about unauthorised surveillance, targeted profiling, data breaches, and intrusive data harvesting have become widespread, putting individuals at considerable risk.[8] Moreover, due to IoT's decentralised and automated nature, users often do not realise which personal data is being collected or how it is used. These features fundamentally challenge traditional privacy protection paradigms, necessitating new regulatory approaches.

Acknowledging these challenges, Kenya passed the Data Protection Act (DPA) in 2019 to improve data governance and safeguard citizens' privacy rights amid

3 Callebaut G., Leenders G., Van Mulders J., Ottoy G., De Strycker L., and Van der Perre L., "The Art of Designing Remote IoT Devices—Technologies and Strategies for a Long Battery Life" (2021) 21 Sensors 913.

4 Khan IH and Javaid Mohd, "Role of Internet of Things (IoT) in Adoption of Industry 4.0" (2021) 07 Journal of Industrial Integration and Management 515

5 Kiaka R.,, "Digital Technology in Kenyan Agriculture: A Scoping Report" (PLAAS 2024) Working paper 67Available at: https://plaas.org.za/wp-content/uploads/2024/05/Working-Paper-67-Digital-Technology-in-Kenyan-Agriculture-Kiaka.pdf (Accessed: 06 October 2025).

6 Aziz Al Kabir M, Elmedany W and Sharif MS, "Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques" (2023) 7 Journal of Cyber Security Technology 199

7 Alam T, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)" (Institute of Electrical and Electronics Engineers (IEEE) 2020) <https://doi.org/10.36227/techrxiv.12657158.v1> accessed October 6, 2025

8 Alaba F. A., Othman M., Hashem I.A.T., and Alotaibi F., "Internet of Things Security: A Surve"', (2017) 88 I 10-28<https:// www.elsevier.com/locate/jnca> accessed on 18 November 2024.

a fast-evolving digital economy.[9] The Act specifies clear responsibilities for data controllers and processors, requires explicit user consent for data processing, and establishes breach notifications and regulatory oversight procedures. Therefore, Kenya's Data Protection Act marks a significant legislative effort to align the country's privacy norms with international best practices, particularly influenced by the European Union's General Data Protection Regulation (GDPR).

Nonetheless, the effectiveness of Kenya's DPA in adequately responding to the distinctive privacy challenges posed by IoT remains uncertain. IoT systems differ fundamentally from conventional digital services, particularly in scale, automation, and the complexity of interactions among interconnected devices. This disparity raises critical questions regarding whether existing legal frameworks sufficiently encompass IoT-specific nuances and whether the provisions of the Data Protection Act adequately address the sophisticated data protection and privacy needs arising from these emerging technologies.[10]

This article aims to critically analyse the effectiveness of Kenya's Data Protection Act in protecting privacy in the context of IoT. It seeks to evaluate both the strengths and weaknesses of existing laws about the practical challenges and complexities of IoT applications in Kenya. Through this analysis, the article aims to identify shortcomings in Kenya's current data protection framework and present actionable recommendations to enhance privacy standards, ensuring that Kenya effectively manages the delicate balance between technological progress and essential privacy rights.

Specifically, the research addresses three primary questions: How has IoT challenged conventional concepts of privacy? To what extent does Kenya's Data Protection Act effectively respond to privacy concerns specific to IoT technology? Lastly, what significant gaps exist in Kenya's legislative framework addressing these concerns?[11] This article not only enhances scholarly insight into privacy regulation in the IoT era but also offers a solid foundation for policymakers, stakeholders, and industry professionals to bolster data protection practices in Kenya. Ultimately, the study highlights the pressing need for Kenya and comparable jurisdictions to proactively revise and improve their legal frameworks to align with fast-paced technological advancements

9 Data Protection Act 2019.

10 Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M , "IoT Privacy and Security: Challenges and Solutions" (2020) 10(12):4102MDIP, AS 4-7 8-10 < https://doi.org/10.3390/app10124102 accessed on 20 September, 2024.

11 Shafiq M., Gu Z., Cheikhrouhou O., Alhakami W., and Hamam H., "The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks" (2022) 2022 *Wireless Communications and Mobile Computing 2-6.*

while protecting citizens' fundamental rights in a connected world.

2.0 Conceptual and Theoretical Framework

Establishing a strong conceptual and theoretical foundation is essential for effectively evaluating Kenya's DPA in tackling IoT ecosystems' privacy and data security challenges. Privacy and protection concepts are relevant to the IoT landscape, and the organised approach offers a clear analytical perspective to assess Kenya's legal provisions' effectiveness systematically.

3.0 Privacy

Privacy, especially regarding IoT, has progressed significantly from traditional notions of individual control over personal information.[12] Today, privacy considerations encompass the processes of data generation, collection, processing, and dissemination within interconnected digital ecosystems. Several dimensions of privacy are relevant to IoT, including information, spatial, decisional, and bodily. Information privacy involves individuals' authority over their data, while spatial privacy pertains to the right to physical and spatial autonomy, which is increasingly challenged by widespread IoT surveillance. Decisional privacy highlights individuals' ability to make choices free from outside interference, and bodily privacy stresses the control over one's physical body and medical information, two areas significantly impacted by IoT devices in healthcare.[13]

Furthermore, data protection principles like consent, data minimisation, transparency, and accountability underpin modern privacy regulations.[14] Consent is vital, demanding that users give clear, informed, and explicit approval before data can be collected or processed.[15] Data minimisation focuses on limiting data collection to what is strictly necessary for specific purposes, thereby lessening the chances of harm from potential data breaches. Transparency entails informing users about how their data is collected, stored, processed, and shared, thus equipping them with knowledge about their personal information's journey. Finally, accountability mandates that organisations managing personal data establish sufficient safeguards and mechanisms to protect privacy proactively, a principle that is becoming

12 Ahmed S and Khan M, "Securing the Internet of Things (IoT): A Comprehensive Study on the Intersection of Cybersecurity, Privacy, and Connectivity in the IoT Ecosystem" (2023) 13 AI, IoT and the Fourth Industrial Revolution Review 1.

13 Ibid.

14 Helm RK, "Conviction by Consent? Vulnerability, Autonomy and Conviction by Guilty Plea" (2019) 83 The Journal of Criminal Law 161

15 European Union General Data Protection Regulation (2016/679).

increasingly crucial in IoT ecosystems.[16]

Safeguarding privacy in IoT settings requires frameworks that integrate privacy aspects into all technology design and implementation stages. The theoretical frameworks and models mentioned below are crucial in shaping international IoT privacy practices and are important benchmarks for this research.

a) Privacy by Design (PbD)

The concept of Privacy by Design (PbD) represents a forward-thinking strategy for privacy management that integrates privacy elements into technologies from the very beginning, rather than applying them after the fact. PbD highlights seven core principles, including a proactive stance over a reactive one, default privacy settings, privacy ingrained in design, positive-sum outcomes with full functionality, end-to-end security, transparency, and respect for user privacy.[17] Implementing PbD principles in IoT development necessitates that device manufacturers and service providers embed privacy safeguards at each phase, thus reducing the privacy risks associated with IoT systems.[18]

b) General Data Protection Regulation (GDPR)-Inspired Frameworks

The GDPR framework has become a global standard, affecting various regions, including Kenya, in developing their data protection regulations. Its core principles are—lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability aim to provide thorough data protection, especially in challenging technological environments such as the Internet of Things (IoT). The extraterritorial reach of the GDPR and its strict compliance requirements present a strong benchmark for evaluating Kenya's legislative approach to IoT privacy issues.[19]

16 Sections 27-36 Data Protection Act 2019.

17 Cavoukian A, "Privacy by Design," Privacy Protection Measures and Technologies in Business Organizations (IGI Global 2012) <https://doi.org/10.4018/978-1-61350-501-4.ch007> accessed October 6, 2025.

18 Perera C. McCormick C., Bandara A.K, Price, B Nuse B, "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms" (2016) 1, *ICIOT 1-9 <https://doi.org/10.48550/arXiv.1609.04060> accessed on 18 August 2024.*

19 Babalola O, "Internet of Things (IoT): Data Security and Privacy Concerns under the General Data Protection Regulation (GDPR)," *Natural Language Processing (Academy and Industry Research Collaboration Center (AIRCC) 2021)* 52-56 <https://doi.org/10.5121/csit.2021.112324> accessed September 1, 2025.

c) Cybersecurity Theoretical Models

Cybersecurity frameworks, like the National Institute of Standards and Technology (NIST) cybersecurity framework (2018), provide thorough guidelines for managing risks linked to interconnected digital devices. Since IoT devices exhibit significant cybersecurity weaknesses that pose a direct risk to personal privacy, cybersecurity theories emphasize the importance of threat identification, vulnerability management, risk assessment, and incident response.[20]

To assess the effectiveness of the DPA in Kenya, it is essential to refer to these cybersecurity best practices, highlighting how well the legislation aligns with or enforces such standards. Drawing from the outlined concepts and theories, the effectiveness of Kenya's Data Protection Act in the IoT context can be evaluated against several distinct yet interrelated criteria:

i. Adequacy of Consent Requirements: Evaluating whether user consent provisions in the DPA accommodate IoT realities, such as automated, continuous data collection.

ii. Enforcement Mechanisms: Analysing the institutional capacity and practicality of enforcing compliance specifically for IoT providers and manufacturers.

iii. Data Minimization and Transparency: Determining how effectively the DPA promotes minimal and transparent data collection practices in IoT implementations.

iv. Security and Breach Notification: Assessing clarity and enforceability of data security and incident reporting obligations within IoT contexts.

v. Compatibility with International Standards: Measuring alignment with international best practices, particularly GDPR and PbD principles, and identifying gaps requiring legislative refinement.

This article will systematically evaluate Kenya's Data Protection Act through conceptual and theoretical lenses, assessing its effectiveness and adaptability to IoT technologies' complex privacy and data protection challenges. This analytical approach provides a thorough understanding of the existing legal framework in Kenya and enables valuable recommendations for improving privacy protection in a more connected and data-driven world.

20 National Institute of Standards and Technology (NIST) cybersecurity framework (2018).

4.0 Overview of IoT and Privacy Concerns

As mentioned above, IoT represents an intricate network comprising physical objects embedded with sensors, software, and connectivity capabilities to facilitate real-time data exchange. By bridging physical and digital domains, IoT fosters environments where devices continuously communicate, collaborate, and operate autonomously. This section critically explores the landscape of IoT adoption in Kenya, highlighting prevalent types of IoT applications, and closely examines the privacy concerns intrinsic to these technologies.[21]

5.0 Adoption and Applications in Kenya

Kenya has emerged as a leading adopter of IoT technology in sub-Saharan Africa in recent years, driven by increasing internet penetration, rapid digitalization efforts, and strategic government initiatives. Prominent examples include innovative city projects such as Nairobi's "Safe City" initiative and Konza Technopolis, illustrating the country's commitment to integrating IoT into urban planning and management.[22] IoT applications in healthcare, such as wearable health monitors and remote patient management systems, demonstrate substantial growth potential and promise transformative improvements in public health services.

Further, Kenya's robust agricultural sector increasingly relies on IoT-enabled precision farming technologies. IoT systems provide farmers with real-time insights into soil quality, moisture levels, and crop health, significantly boosting yields and optimizing resource use. Similarly, IoT deployment in energy management and environmental monitoring, notably in wildlife conservation

21 Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations" (2019). *IEEE, 21(3), 2702–2733. <https://doi.org/10.1109/COMST.2019.2910750> accessed on 16 December, 2024.several surveys were put forward addressing various IoT-centric topics, including intrusion detection systems, threat modeling, and emerging technologies. In contrast, in this paper, we exclusively focus on the ever-evolving IoT vulnerabilities. In this context, we initially provide a comprehensive classification of state-of-the-art surveys, which address various dimensions of the IoT paradigm. This aims at facilitating IoT research endeavors by amalgamating, comparing, and contrasting dispersed research contributions. Subsequently, we provide a unique taxonomy, which sheds the light on IoT vulnerabilities, their attack vectors, impacts on numerous security objectives, attacks which exploit such vulnerabilities, corresponding remediation methodologies and currently offered operational cyber security capabilities to infer and monitor such weaknesses. This aims at providing the reader with a multidimensional research perspective related to IoT vulnerabilities, including their technical details and consequences, which is postulated to be leveraged for remediation objectives. Additionally, motivated by the lack of empirical (and malicious*

22 Manoharan P Nagarathinam S.,and Ramakrish V.P, "Keep It Open, Keep It Safe," *Proceedings of the 7th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation* (ACM 2020) <https://doi.org/10.1145/3408308.3427618> accessed October 6, 2025.

and anti-poaching operations, illustrates Kenya's creative adaptation of technology to solve unique national challenges.[23]

However, alongside these beneficial applications, IoT's pervasive integration into daily life inevitably amplifies data privacy and security risks. This multifaceted integration necessitates careful consideration of its implications on privacy norms and expectations.

IoT devices continuously generate and collect vast amounts of data, often operating unobtrusively in the background, beyond explicit user awareness or control. Unlike conventional computing technologies, IoT data collection usually lacks transparent mechanisms for users to fully comprehend or manage their personal information.[24] Data types commonly collected include location coordinates, biometric identifiers, health metrics, environmental conditions, and behavioural patterns.[25]

Moreover, IoT ecosystems typically involve extensive data sharing among diverse stakeholders, including device manufacturers, cloud storage providers, third-party analytics services, and governmental entities. IoT systems automated, decentralized, and heterogeneous nature makes traditional models of informed user consent and data minimization difficult to apply effectively.[26]

Furthermore, IoT devices frequently employ cloud computing and third-party services, complicating compliance with local data protection laws, especially regarding cross-border data transfers. Such dynamics underscore significant vulnerabilities in managing data privacy effectively within IoT infrastructures.

23 Ibid.

24 Sudha R., Pooja G., Revathy V., and Dilip Kumar S.,, "Enhanced Data Privacy Using Vertical Fragmentation and Data Anonymization Techniques," *Advances in Parallel Computing* (IOS Press 2021) <https://doi.org/10.3233/apc210292> accessed October 6, 2025.

25 Brass I., and Sowell J. H., "Adaptive Governance for the Internet of Things: Coping with Emerging Security Risks" (2021) 15 Regulation & Governance 1092-1110 < https://doi.org/10.1111/rego.12343> accessed on 12 March 2025.

26 Fagan M., Megas k.,Marron J.,Link E.,Brady K.,Cuthill B., "IoT Device Cybersecurity Guidance for the Federal Government : IoT Device Cybersecurity Requirement Catalog" (National Institute of Standards and Technology (US) 2021) NIST SP 800-213A <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf> accessed 27 March 2025.

6.0 Privacy Risks and Concerns in IoT

IoT technologies introduce several unique and significant privacy risks, broadly categorized as follows:

a. *Unauthorized Surveillance and Monitoring*

IoT devices equipped with cameras, microphones, or geolocation capabilities can facilitate unauthorized surveillance, infringing upon individuals' privacy expectations. Instances of unauthorized data collection by smart-home devices or covert monitoring through IoT-powered security cameras exemplify how IoT ecosystems potentially expose individuals to persistent monitoring without explicit consent or knowledge.[27]

b. *Data Breaches and Security Vulnerabilities*

IoT devices are notoriously susceptible to security breaches due to inherent weaknesses in hardware design, software vulnerabilities, inadequate security updates, and weak authentication protocols. Breaches of IoT data can expose sensitive personal information, including biometric data and health records, heightening risks of identity theft, extortion, and loss of confidentiality. Such breaches pose pronounced threats in critical sectors like healthcare, where compromised IoT devices could significantly harm individuals' well-being or privacy.[28]

c. *Profiling and Intrusive Analytics*

The continuous collection and aggregation of IoT-generated data enable sophisticated profiling of individuals based on their behaviours, routines, health status, or preferences. Such profiles may result in intrusive targeting, discriminatory practices, and manipulation by entities capable of deriving inferences from aggregated data. The opacity of data flows exacerbates the potential misuse or unauthorized exploitation of user data, compromising individual autonomy and decisional privacy.[29]

27 Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M , "IoT Privacy and Security: Challenges and Solutions" (2020) 10(12):4102MDIP, AS 4-7 8-10 < https://doi.org/10.3390/app10124102 accessed on 20 September, 2024.

28 Sun P, "A Survey on Privacy and Security Issues in IoT-Based Environments: Technologies, Protection Measures and Future Directions" (2025) 148 Computers & Security 104097 https://doi.org/10.1016/j.cose.2024.104097 accessed 30th August, 2025.

29 Kanniappan J and Rajendiran B, "Privacy in the Internet of Things," *Censorship, Surveillance, and*

d. Inadequate Consent Mechanisms

Traditional consent frameworks, requiring explicit approval at each data-collection point, are often incompatible with IoT devices, which collect data unobtrusively and continuously. Frequently, consent processes in IoT applications are either inadequately implemented or absent, with users having limited awareness or understanding of data collection practices, purposes, or downstream uses.

In Kenya, these general IoT-related privacy challenges are amplified by specific contextual issues, including limited public awareness of privacy rights, weak enforcement capabilities, and uneven technological literacy among the population. Additionally, Kenya's emerging IoT market often involves multinational technology companies whose data-handling practices may diverge significantly from local data protection expectations, complicating compliance and enforcement.[30]

The growing presence of international IoT players, the prevalence of cross-border data transfers, and limited domestic technical expertise compound these privacy challenges, necessitating robust legal frameworks and enforcement mechanisms tailored to Kenya's unique socio-technological context.[31]

The complex interplay between technological advancement, expansive data generation, and privacy protection underscores the need to reassess and fortify regulatory frameworks governing data privacy within IoT ecosystems. Kenya's current trajectory toward widespread IoT adoption offers tremendous potential for socioeconomic development yet simultaneously presents substantial privacy risks requiring careful management.[32] This overview has thus highlighted the pressing necessity of a thorough legal evaluation to understand how Kenya's Data Protection Act currently responds to these intricate challenges,

Privacy (IGI Global 2019) 7-12 <https://doi.org/10.4018/978-1-5225-7113-1.ch077> accessed September 1, 2025

30 Babalola O, "Internet of Things (IoT): Data Security and Privacy Concerns under the General Data Protection Regulation (GDPR)," *Natural Language Processing (Academy and Industry Research Collaboration Center (AIRCC) 2021)* 52-56 <https://doi.org/10.5121/csit.2021.112324> accessed September 1, 2025

31 Javanmardi S., Nascita A., Pescapè A., Merlino G., and Scarpa M., "An Integration Perspective of Security, Privacy, and Resource Efficiency in IoT-Fog Networks: A Comprehensive Survey" (2025) 270 *Computer Networks 111470*.

32 Ziegeldorf JH, Morchon OG and Wehrle K, "Privacy in the Internet of Things: Threats and Challenges" (2013) 7 *Security and Communication Networks 2728*.

thereby laying the groundwork for assessing regulatory effectiveness in subsequent sections of this article.

7.0 Analysis of Kenya's Data Protection Act, 2019

The implementation of the DPA represented a pivotal moment in the country's digital governance landscape. The Act seeks to safeguard personal data privacy within a rapidly digitizing society. With the rise of IoT technologies in various sectors, this section examines the provisions of the Act, assessing their sufficiency, relevance, and the practicality of enforcement in tackling IoT-related privacy issues. This analysis offers insights into both the strengths and the fundamental weaknesses of the current legislative framework.[33]

The Data Protection Act of 2019 establishes a comprehensive legal framework addressing several critical areas relevant to IoT privacy concerns:

a. Obligations of Data Controllers and Data Processors

Under the DPA, entities collecting, processing, or managing personal data are classified as data controllers or processors, each with distinct obligations. Data controllers typically IoT device manufacturers, service providers, or application developers are primarily responsible for compliance with data protection principles, including lawful processing, data minimization, transparency, and accuracy.[34] Data processors entities performing processing on behalf of controllers must adhere strictly to the controllers' instructions, implement security safeguards, and assist in ensuring compliance with the Act's requirements.[35]

b. User Consent Requirements

The DPA stipulates explicit consent as a fundamental requirement for processing personal data. Section 30 specifies that data subjects must give informed, freely provided, and explicit consent before data processing. This provision underscores the importance of transparency and control over personal data, factors directly challenged by the automated and continuous nature of data collection typical in IoT ecosystems.[36]

33 Sun P, "A Survey on Privacy and Security Issues in IoT-Based Environments: Technologies, Protection Measures and Future Directions" (2025) 148 Computers & Security 104097 https://doi.org/10.1016/j.cose.2024.104097 accessed 30th August, 2025.

34 Section 25, DPA.

35 Section 42 DPA

36 Note 7.

c. Data Minimization and Purpose Limitation

Data minimization principles, outlined under Section 25, emphasise that data collection should be strictly limited to what is necessary for clearly defined and lawful purposes. The DPA prohibits excessive or unnecessary data collection, potentially addressing privacy concerns arising from the vast, continuous streams of personal data collected by IoT devices.[37]

d. Security and Breach Notification Obligations

Sections 41 and 43 of the DPA specifically mandate data controllers and processors to adopt appropriate security measures and to report data breaches to the Office of the Data Protection Commissioner (ODPC) within a prescribed period. This is particularly significant for IoT, where devices' inherent security vulnerabilities can significantly amplify risks to personal data security.[38]

e. Establishment and Role of the Office of the Data Protection Commissioner (ODPC)

The ODPC, established under Section 5, is the primary oversight and enforcement authority, supervising data protection compliance, investigating complaints, and issuing administrative penalties or sanctions for violations. Its effectiveness directly impacts the enforceability of privacy standards in IoT applications.[39]

8.0 Strengths and Weaknesses

Kenya's DPA aligns significantly with international best practices, notably mirroring the EU's GDPR principles. This alignment facilitates compliance among multinational IoT enterprises and enhances Kenya's attractiveness for global technological investments. The DPA addresses several foundational privacy concerns exacerbated by IoT technologies by explicitly covering consent, transparency, purpose limitation, and data minimisation. The Act's strong emphasis on informed consent and clear user rights supports efforts to ensure meaningful user autonomy in IoT contexts.[40]

Explicit obligations to report data breaches promptly and implement security measures proactively represent an important step in recognising IoT-

37 Section 25 DPA.
38 Note 7.
39 Note 7.
40 Note 19.

related security vulnerabilities. These provisions can significantly enhance accountability and prompt action in case of data compromises. Despite notable strengths, the DPA has limitations when explicitly applied to IoT technologies. The DPA's explicit consent requirements present practical challenges when applied to IoT environments. Given IoT's continuous, automated, and often passive data collection, it remains unclear how controllers should implement continuous consent mechanisms effectively without causing consent fatigue or impractical user interactions.

IoT devices commonly rely on cloud services involving cross-border data transfers. However, Section 48, which governs cross-border data flows, provides general guidelines without explicit detail concerning IoT-specific scenarios. This lack of clarity could compromise compliance and enforcement regarding IoT devices that store or process data internationally.[41]

The ODPC, tasked with ensuring compliance, faces resource constraints and limited technical capacity in monitoring complex, diverse, and dispersed IoT ecosystems. The effectiveness of privacy protection hinges on the ODPC's capability to understand IoT-specific technologies and adequately enforce the provisions of the DPA, an area currently underdeveloped.

Although the DPA mandates appropriate data security measures, it offers little explicit guidance concerning security standards specific to IoT hardware and software vulnerabilities. Given IoT devices' well-documented susceptibility to cyber threats, more explicit statutory guidance on minimum security standards is necessary.

The preceding analysis indicates that the DPA exhibits ambiguity in enforcing informed and continuous consent requirements in IoT contexts. Furthermore, adequate guidance concerning cross-border data transfers relevant to IoT applications is lacking.[42] Additionally, explicit security standards specifically addressing IoT device vulnerabilities are missing, along with institutional constraints within the ODPC that hinder effective oversight and enforcement.

These gaps underscore the necessity for targeted legislative amendments, enhanced regulatory guidance, and institutional capacity-building to ensure robust and practical privacy protections in Kenya's expanding IoT landscape.[43]

41 Singh DrS and Prerna, "Regulation Of Cross-Border Data Flow And Its Privacy In The Digital Era" (2024) 9 *NUJS Journal of Regulatory Studies* 40, 43.

42 Meltzer J, "The Internet, Cross-Border Data Flows and International Trade" [2013] *SSRN Electronic Journal* 90-102 <10.1002/app5.60> accessed 1st September, 2025.

43 Consulting D, "Comparing Kenya Data Protection Act 2019 to EU GDPR" (DataHub Consulting, March 6, 2024) <https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/> accessed September 2, 2025.

DPA constitutes a significant legislative advancement toward comprehensive personal data protection, effectively addressing numerous general privacy concerns. Nevertheless, specific practical and interpretative shortcomings remain prominent within the context of IoT. Addressing these gaps proactively will be essential to safeguarding privacy in the continuously evolving digital environment shaped significantly by IoT technologies. Future legal and policy developments should explicitly reflect the nuances of IoT privacy and security risks, reinforcing the Act's robustness and responsiveness to emerging technological realities.

9.0 Case Studies

9.01 Smart City Initiatives—Konza Technopolis and Nairobi's Safe City Project

Kenya has ambitiously pursued IoT-driven smart city initiatives to enhance urban efficiency, safety, and sustainability. Two prominent examples are Konza Technopolis a government-backed futuristic city, and Nairobi's Safe City Project, which deploys IoT-powered surveillance infrastructure to enhance public security.[44]

Konza Technopolis seeks to utilise IoT for urban management by incorporating smart sensors for traffic regulation, automated waste disposal, and enhanced public safety oversight. These IoT systems gather extensive personal and environmental data continuously.

While the DPA requires transparent consent processes and strict data minimisation, implementing this in extensive urban settings presents considerable obstacles. The ongoing and unrestricted nature of data collection by smart city sensors adds complexity to following the Act's specific consent requirements. Currently, the DPA does not provide comprehensive guidelines for continuous and automated consent processes, resulting in possible conflicts between effective IoT implementation and adherence to regulations.

Nairobi's Safe City Project, which includes widespread CCTV installations and IoT-driven facial recognition systems, presents significant privacy issues from surveillance. Although security advantages exist, ongoing surveillance may unintentionally violate individuals' privacy rights, in contravention of the DPA, which

44 Rattan S and Jeet Kaur DrM, "IoT in Smart Cities," Key Insights from Harnessing AI, Machine Learning, and IoT for Smart Business (Iterative International Publishers, Selfypage Developers Pvt Ltd 2025) <https://doi.org/10.58532/nbennurkich2> accessed October 6, 2025.

stresses the need for explicit and informed consent.[45] The lack of transparency regarding data collection methods, retention durations, and data sharing with law enforcement agencies highlights serious enforcement deficiencies and inadequate institutional oversight by the ODPC. These initiatives reveal significant enforcement challenges due to unclear provisions in the Act and emphasise the need for specific regulatory guidance that addresses innovative city applications.

9.02 Healthcare IoT

In Kenya, the healthcare sector quickly embraces IoT technology, particularly through wearable health-monitoring devices and remote patient management systems. This includes devices such as wearable glucose monitors, heart-rate trackers, and telemedicine applications that facilitate healthcare professionals' real-time monitoring of patients. [46]

Although these advancements enhance healthcare accessibility and service delivery, they raise serious concerns regarding data privacy. Wearable health devices collect sensitive biometric and medical information continuously, which can infringe on privacy if the data is not securely protected or is improperly shared with third parties.[47] The Data Protection Act mandates informed consent, strong data security protocols, and transparent practices for data sharing.[48]

However, the practical application of these regulations within healthcare IoT is fraught with challenges. For example, the ongoing nature of data collection complicates the management of explicit consent, often resulting in vague or ambiguous consent methods that do not meet the DPA's strict standards.

Moreover, healthcare IoT often entails cross-border data transfers for cloud storage or analytics services from international companies. According to the DPA, such transfers necessitate clear consent and conditions of data protection equivalence, which are routinely

45 Section 30 DPA.

46 Abdulmalek S, Nasir A, Jabbar WA, Almuhaya MAM, Bairagi AK, Khan MA, Kee SH., "IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review" (2022) 10 Healthcare 1993.

47 Chunyan Li, Jiaji Wang, Shuihua Wang , Yudong Zhang, "A review of IoT applications in healthcare", (2024), Neurocomputing, 565, 127017, ISSN 0925-2312, https://doi.org/10.1016/j.neucom.2023.127017 accessed 6th October, 2025.

48 Sections 25 and 41 DPA.

neglected or poorly handled in practice due to the limited technological understanding among patients and healthcare providers.[49] Enforcement challenges arise from the ODPC's limited technical capacity to effectively regulate the complexities of healthcare-specific IoT, increasing the risks of privacy violations and the misuse or compromise of sensitive personal data.

9.03 Agricultural IoT

Agriculture is vital to Kenya's economy and increasingly depends on IoT-driven precision farming technologies. Common IoT devices in agriculture include soil moisture sensors, automated irrigation systems, livestock tracking gadgets, and drones for crop observation. These tools gather and analyse vast amounts of data regarding farming conditions, livestock well-being, and productivity metrics, often encompassing personal information about farmers and their practices.[50]

Although precision agriculture significantly enhances productivity and efficiency, it raises considerable data privacy issues. IoT devices can unintentionally gather sensitive information such as exact location data, personal financial details, and farming methods. Data protection awareness among smallholder farmers, who comprise most of Kenya's agricultural sector, is notably low. This lack of awareness leads to an insufficient understanding of data privacy rights and the risks of sharing information with third-party agrarian firms.[51]

The Data Protection Act mandates explicit consent, transparency, and minimal data collection which pose practical challenges in this agricultural setting. Many agricultural IoT solutions fail to inform farmers about data processing practices, compromising transparency and informed consent.[52] Moreover, farmers generally do not have control over their data after it is collected, increasing the risk of unauthorised commercial use or targeted marketing by agricultural suppliers. Additionally, the ODPC's limited rural outreach and

49 Ibid.

50 Antony, A.P.; Leith, K.; Jolley, C.; Lu, J.; Sweeney, D.J. "A Review of Practice and Implementation of the Internet of Things (IoT) for Smallholder Agriculture" Sustainability 2020, 12, 3750. https://doi.org/10.3390/su12093750> accessed 6 October, 2025.

51 Strathmore University and iLabAfrica, "Empowering Smallholder Farmers Through IoT and AI - @iLabAfrica" (@iLabAfrica - Changing Lives Through Research and Innovation, February 29, 2024) <https://ilabafrica.strathmore.edu/empowering-smallholder-farmers-through-iot-and-ai/> accessed October 6, 2025

52 Sections 25 and 30 DPA.

enforcement efforts further heighten these vulnerabilities, highlighting significant institutional and educational weaknesses within Kenya's current data protection landscape.

These detailed case studies vividly illustrate that, while Kenya's Data Protection Act provides a theoretically robust foundation for data privacy, practical application in IoT-specific contexts reveals significant compliance gaps and enforcement challenges.

Addressing these practical issues requires targeted legislative enhancements, more straightforward regulatory guidelines, substantial institutional capacity-building, and proactive public education initiatives. Such improvements will significantly enhance the Act's practical effectiveness, positioning Kenya to harness IoT technologies safely and ethically, with robust safeguards protecting citizens' fundamental privacy rights.[53]

8.04 Comparative Legal Analysis

The GDPR, enforced since 2018, represents the most influential global standard for data protection. It explicitly addresses modern digital privacy challenges, offering comprehensive and robust protections relevant to IoT contexts.

a. Consent Requirements and IoT

GDPR mandates explicit, informed, and freely given consent emphasising transparency and clarity regarding data collection purposes and processes. Unlike Kenya's DPA, GDPR provides clear guidelines for consent management in digital environments, including dynamic scenarios prevalent in IoT. For example, GDPR emphasises data controllers' responsibility to continuously inform users of changes in data collection practices, promoting meaningful consent through privacy dashboards, periodic notifications, and straightforward consent revocation methods.[54]

53 Itotia S, Muriithi B. Gitahi S., Korir P., Murigi M., Olukuru J and Sevilla J., "Enhancing Agricultural Support for Small Scale Farmers in Kenya: An IoT-Based Mini Weather Station as a Machine Learning Data Collector," 2023 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT) (IEEE 2023) <https://doi.org/10.1109/gcaiot61060.2023.10385094> accessed October 6, 2025

54 Article 7 GDPR

b. Data Minimisation and Purpose Limitation

GDPR enforces stringent data minimisation explicitly demanding that data collected must be strictly limited to what is necessary for a clearly defined purpose. Moreover, it requires data controllers to periodically justify ongoing data collection and retention practices, which is particularly significant in IoT scenarios involving extensive, real-time data collection. This clear and explicit requirement exceeds the relatively general guidelines provided by Kenya's DPA, offering a robust framework to manage IoT-generated data.[55]

c. Cross-border Data Transfers and IoT

Under GDPR strict provisions govern cross-border data transfers, explicitly mandating the adequacy of data protection standards in recipient jurisdictions. GDPR provides mechanisms such as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs), offering clear guidelines for compliance in international IoT data-sharing contexts. Kenya's DPA, in contrast, provides limited explicit guidance, revealing a significant gap that complicates cross-border IoT data flows.[56]

d. Institutional Enforcement and Accountability

GDPR emphasises institutional accountability through dedicated supervisory authorities empowered to impose significant financial penalties (up to 4% of annual global turnover) for non-compliance.[57] This strong enforcement mechanism and mandatory Data Protection Impact Assessments (DPIAs) for high-risk processing protect personal data privacy in IoT contexts. Kenya's ODPC remains under-resourced, and its penalties are considerably lower, limiting deterrence and effective enforcement.[58]

10.0 South Africa's Protection of Personal Information Act (POPIA)

South Africa's POPIA, enacted in 2013 and enforced from 2021, shares significant similarities with Kenya's DPA but provides notable distinctions and clarifications advantageous to IoT contexts.[59]

55 Article 5 GDPR.
56 Articles 44-50 GDPR.
57 Articles 83-84 GDPR.
58 Article 35 GDPR.
59 Protection of Personal Information Act (POPIA),

a. Comprehensive and Clear Definitions

POPIA explicitly defines sensitive categories of personal information, clarifying protections around biometric and health data, which is highly relevant in IoT contexts. Clear definitions reduce ambiguity in compliance obligations, enhancing effective data protection implementation, a specificity lacking in Kenya's DPA, potentially leading to interpretative ambiguities.[60]

Consent Flexibility for Continuous Data Collection

POPIA acknowledges scenarios where continuous consent is impractical and allows broader, purpose-specific consent complemented by rigorous transparency requirements.

This pragmatic consent framework is particularly suitable for IoT environments, offering flexibility balanced by strict transparency and accountability provisions. Kenya's DPA, by contrast, lacks equivalent flexibility, complicating practical implementation in continuous IoT data collection scenarios.

b. Robust Security Safeguards and Breach Notification

POPIA's security provisions are notably detailed, requiring comprehensive, reasonable measures based on internationally recognised standards to protect personal data. It also mandates immediate notification of data breaches to regulators and affected data subjects, a stringent and transparent approach, especially critical for IoT. In comparison, Kenya's DPA offers less specificity regarding IoT security standards, leaving implementation vulnerable to interpretation and non-compliance.[61]

c. Institutional Capacity and Enforcement

POPIA established the Information Regulator, a well-resourced, independent enforcement body with clearly delineated authority to investigate violations, impose substantial penalties, and promote public awareness about data protection rights.

By contrast, Kenya's ODPC remains institutionally constrained by

60 Cornelius FP and Jansen van Rensburg SK, "Emerging South African Smart Cities: Data Security and Privacy Risks and Challenges" (2024) 26 *South African Journal of Information Management 36,39.*

61 Myeko Z and Rambe P, "IoT Appropriation for Crop Management and Productivity Enhancement in South Africa" (2024) 26 *South African Journal of Information Management 1-5.*

limited technical capacity and inadequate resources, reducing its efficacy in enforcing IoT-specific compliance effectively.[62]

11.0 Lessons and Best Practices for Kenya's Data Protection Framework

The comparative analysis with GDPR and POPIA highlights critical lessons and best practices that could significantly enhance Kenya's Data Protection Act in managing IoT-specific privacy concerns effectively:

a. Explicit Guidelines for Continuous and Dynamic Consent: Adopting clear regulatory guidelines for managing continuous consent, as GDPR and POPIA exemplify, would mitigate consent management ambiguities inherent in IoT environments.

b. Clear and Detailed Cross-border Data Transfer Provisions: Developing specific and explicit cross-border data transfer guidelines, similar to GDPR's Binding Corporate Rules and Standard Contractual Clauses, would significantly enhance compliance clarity for IoT implementations.

c. Enhanced Data Minimisation and Transparency Requirements: Clear and explicit obligations for data controllers to regularly justify data collection and retention would reinforce transparency and accountability within Kenya's IoT ecosystem.

d. Strengthened Institutional Capacity and Enforcement Powers: Strengthening ODPC's institutional and technical capacity and increasing penalties for non-compliance would greatly enhance regulatory oversight and enforcement effectiveness, aligning more closely with international best practices demonstrated by GDPR and POPIA.

This comparative analysis shows that while Kenya's Data Protection Act aligns well in principle with global data protection frameworks, significant gaps and ambiguities limit its practical effectiveness in addressing IoT-specific privacy challenges. Kenya can significantly enhance its legal framework's robustness by adopting more precise consent mechanisms, explicit cross-border data transfer rules, rigorous data minimisation and transparency standards, and bolstered institutional enforcement capacity.

62 Komna L and Mpungose S, "Investigating the Challenges to Digital Transformation in the Public Sector, A Case Study of the State Information Technology Agency (SITA), South Africa" (2024) 15 HOLISTICA – *Journal of Business and Public Administration 15, 18.*

Integrating these best practices will ensure adequate protection of citizens' privacy rights amidst the rapid proliferation of IoT technologies.

12.0 Recommendations

Based on the preceding analysis and practical insights from case studies and international comparisons, this section provides targeted recommendations to significantly enhance Kenya's Data Protection Act (DPA) in addressing IoT-specific privacy concerns. These recommendations encompass legislative refinements, regulatory enhancements, strengthened enforcement mechanisms, and institutional capacity-building, collectively robustly positioning Kenya's legal framework to protect data privacy in the connected age.

a. *Legislative Amendments and Clarifications*

The dynamic, automated nature of data collection through IoT devices necessitates legislative changes that explicitly address continuous consent mechanisms. The Data Protection Authority (DPA) should implement provisions akin to those in the GDPR, clearly defining methods for obtaining, managing, and periodically reaffirming consent within IoT ecosystems. These provisions might encompass clear guidelines on layered consent mechanisms, simplified privacy notices, and digital dashboards that empower users to manage their consent preferences actively.

Considering the fundamental reliance of IoT technologies on international cloud services and data-sharing arrangements, explicit regulations governing cross-border data transfers are essential. The Act should incorporate comprehensive mechanisms similar to GDPR's Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). These guidelines would detail the conditions under which cross-border transfers are allowed, ensuring that international data exchanges involving IoT comply with Kenya's data protection norms.

To effectively tackle IoT-specific vulnerabilities, the DPA should mandate adherence to internationally recognised IoT security standards, such as those set by NIST or ISO. Including specific requirements for manufacturers and IoT service providers to conduct regular security audits, penetration testing, and security assessments can greatly reduce vulnerabilities and bolster data protection.[63]

63 "5 Years of the Data Protection Act: Progress, Challenges, and the Road Ahead" (*Amnesty Kenya*, January 21, 2025) <https://www.amnestykenya.org/5-years-of-the-data-protection-act/> accessed

b. Regulatory Enhancements and Guidelines

The Office of the Data Protection Commissioner (ODPC) should develop and disseminate comprehensive regulatory guidelines addressing IoT privacy risks. This guidance should outline detailed compliance expectations, practical data-minimisation strategies, recommended consent-management frameworks, security best practices, and precise mechanisms for breach reporting in IoT contexts.[64]

The ODPC should explicitly require mandatory DPIAs for high-risk IoT deployments, including smart-city projects, healthcare devices, and precision agriculture. Regular DPIAs would proactively identify privacy risks, ensure compliance with privacy-by-design principles, and enhance accountability among IoT providers and manufacturers.

c. Strengthening Institutional Capacity

Effectively regulating IoT requires significant technical expertise. The Kenyan government should allocate resources to recruit skilled technical professionals with specialised knowledge in cybersecurity, IoT systems, data analytics, and privacy management.

Enhancing ODPC's technical capacity would significantly improve oversight and enforcement capabilities, enabling proactive responses to emerging privacy threats. Limited resources and insufficient deterrent penalties constrain ODPC's current enforcement capabilities. Enhancing ODPC's enforcement resources, including budget allocations, technical infrastructure, and investigative powers, alongside significantly increasing penalties for non-compliance, would substantially improve regulatory compliance among IoT stakeholders.[65]

The ODPC should establish a dedicated unit that oversees compliance within the IoT sector. This specialised unit would conduct audits, investigations, and educational outreach programs, ensuring focused and continuous oversight of IoT privacy practices.

October 6, 2025.

64 Ibid.

65 "Data Privacy and Protection in Kenya: A Regulatory Review - Financial Sector Deepening Kenya" (*FSD Kenya*, January 28, 2022) <https://www.fsdkenya.org/blogs-publications/data-privacy-and-protection-in-kenya-a-regulatory-review/> accessed October 6, 2025.

d. Enhancing Public Awareness and Education

Recognising the limited public awareness of data protection rights, the ODPC should initiate nationwide campaigns to educate citizens about IoT privacy risks and data protection rights. These campaigns would utilise various communication channels, including digital platforms, media broadcasts, community workshops, and school programs, significantly increasing public knowledge and empowerment regarding IoT privacy rights.[66]

ODPC, in collaboration with academic institutions and industry associations, should establish training and certification programs for IoT device manufacturers, software developers, and data processors. These programs would ensure stakeholders understand their obligations clearly, adhere to best privacy and data protection practices, and remain updated on legislative and technological developments.

e. Promoting Industry Collaboration and Self-Regulation

The ODPC should encourage industry stakeholders to adopt voluntary privacy codes of conduct tailored to IoT contexts. These industry-driven frameworks, overseen by ODPC, would establish self-regulatory standards complementing statutory requirements, further enhancing practical compliance with privacy protection measures.[67]

Public-private partnerships should be encouraged to address IoT-specific privacy challenges through collaborative innovation. Government bodies, private sector entities, academia, and civil society should collaborate to research, develop, and pilot privacy-enhancing technologies (PETs), consent management innovations, and security frameworks tailored explicitly for the IoT ecosystem.

f. Periodic Legislative Review and Adaptation

In light of the swift technological advancements, the Kenyan Parliament should create systems for ongoing legislative evaluations of the Data Protection Act.

66 Ibid.

67 Amnesty Kenya, "5 Years of the Data Protection Act: Progress, Challenges, and the Road Ahead" (*Amnesty Kenya*, January 21, 2025) <https://www.amnestykenya.org/5-years-of-the-data-protection-act/> accessed October 6, 2025.

Regular reviews, guided by public feedback, expert analyses, and emerging technological trends, will guarantee that the Act remains flexible, strong, and relevant in tackling new privacy issues related to IoT.[68]

A specialised advisory committee of legal professionals, technologists, industry experts, and civil society members should be established to track developments in IoT and other innovative technologies continuously. The committee's expertise would direct amendments to laws and regulations, helping to maintain Kenya's data protection framework as proactive and future oriented.[69]

Adopting these recommendations comprehensively would greatly improve the efficacy of Kenya's Data Protection Act in addressing IoT-related privacy and data security challenges. Key measures include legislative updates, clearer regulatory frameworks, strong enforcement practices, increased institutional capacity, widespread public education initiatives, and collaborative efforts among stakeholders, all vital for protecting personal data in Kenya's connected environment.[70] Together, these strategies will establish Kenya as a regional frontrunner in data protection, promoting ongoing technological progress while upholding citizens' essential privacy rights.[71]

13.0 Conclusion

The swift integration of Internet of Things (IoT) technologies has significantly changed contemporary societies, opening new avenues for innovation, efficiency, and economic development. Kenya, propelled by projects like Konza Technopolis, Nairobi's Safe City, healthcare digitisation, and precision agriculture, is at the leading edge of IoT adoption in sub-Saharan Africa. However, this technological shift has serious implications for privacy and data protection, putting pressure on existing regulatory frameworks established for less complex digital scenarios.

68 Sahu S.K and Mazumdar K., "Exploring Security Threats and Solutions Techniques for Internet of Things (IoT): From Vulnerabilities to Vigilance" (2024) 7 *Frontiers in Artificial Intelligence 1397480.*

69 Taeihagh A., Ramesh M. and Howlett M., "Assessing the Regulatory Challenges of Emerging Disruptive Technologies" (2021) 15 Regulation & Governance 1009 2, 4, 5, and 7 <https://doi.org/10.1111/rego.12392> accessed on 6 March 2025.

70 Ngoepe M., and Ngwenya M., "Personal Data and the Assemblage Security in Consumer Internet of Things" (2022) 16 (1) (IJISP) 2,3,4,5,6. https://doi.org/10.4018/IJISP.2022010108 accessed on 17 January 2025.

71 Akamanzi C, Akamanzi, Deutscher P., Guerich B.,| Lobelle A, Ooko-Ombaka A, "Silicon Savannah: The Kenya ICT Services Cluster" *Microeconomics of Competitiveness* (2016) 1, 23, 27-30.

To tackle these privacy challenges, Kenya implemented the Data Protection Act (DPA) in 2019, which outlines a strong legislative structure closely aligned with international standards, especially the EU's GDPR. This article illustrates that the DPA encompasses vital data protection principles, such as explicit consent, data minimisation, transparency, and accountability, placing Kenya well ahead in the regional landscape. Despite its progressive nature, the effectiveness of the Act in addressing IoT-specific privacy issues exposes considerable practical and interpretative hurdles, underscoring the need for ongoing review and adaptation.

Through comprehensive analyses and case studies related to Kenya's smart city projects, healthcare initiatives, and agricultural applications, it becomes clear that the theoretical advantages of the Act encounter significant obstacles in practical application. Notable challenges include managing ongoing and automated consent, uncertainties surrounding cross-border data transfers, insufficient detail regarding IoT security mandates, and serious limitations in the Office of the Data Protection Commissioner (ODPC) enforcement capabilities. Additionally, comparisons with globally recognised frameworks such as GDPR and South Africa's POPIA further highlight these shortcomings, revealing valuable insights and effective international practices Kenya could adopt to enhance its regulatory framework.

As a result, the article offers a range of targeted recommendations aimed at legislative improvement, regulatory strengthening, enhanced institutional enforcement capabilities, and substantial investments in public education and awareness. Specifically, recommended measures include clear guidelines for managing continuous consent in IoT contexts, established frameworks for cross-border data transfers, definitive security standards, obligatory Data Protection Impact Assessments (DPIAs), bolstered institutional capacity for the ODPC, and proactive public-private partnerships.

Furthermore, consistent legislative reviews, guided by expert advisory groups on emerging technologies, will help ensure the Act remains adaptable to rapid technological changes.

The main conclusion of this study stresses that effectively addressing IoT privacy challenges demands flexible, multifaceted strategies rather than fixed, universal legislative answers. While Kenya's current Data Protection Act serves as a crucial foundation, significant improvements are necessary to navigate the complexities of IoT privacy effectively.

Legislative precision improved regulatory guidance, strong institutional enforcement, extensive public awareness, and proactive stakeholder partnerships are crucial components for a resilient, future-ready data protection framework in Kenya.

By adopting these proposed measures, Kenya not only safeguards its citizens' privacy rights but also positions itself as a regional frontrunner in data governance and privacy protection in the era of connectivity. Ultimately, a proactive and ongoing regulatory evolution will empower Kenya to reap the socio-economic advantages of IoT technologies while securely upholding fundamental human rights related to privacy and data protection.

Data Protection and Privacy Compliance for Schools in Kenya

Mafrick Munene*[1]

Abstract

The Data Protection Act, 2019 (DPA) is the primary and comprehensive data protection statute covering both the private and public sectors. The Act was enacted to operationalize Article 31 (c) and (d) of the Constitution, 2010. The Data Protection Regulations, 2021, were also enacted to help in the practical implementation of the Act for data handlers (data controllers and data processors). The Act sets up the Office of the Data Protection Commissioner (ODPC) as the regulator to register, regulate personal data processing, and protect individual privacy, and provide data subjects with rights and remedies to safeguard breaches of their personal data. The terms 'data protection' and 'data privacy' are used interchangeably to mean the same thing. But in a strict sense, the two terms mean two different things in their concepts. The focus of this article is to highlight the key personal data concepts and outline the general framework for compliance for schools in line with the principles of data protection and privacy. The article starts by introducing the subject, proceeds to look at the schools as data controllers and processors, the legal and regulatory framework, data subjects and their rights, and expounds on the principles of personal data protection, compliance requirements, and the role of the Office of the Data Protection Commissioner (ODPC) in assisting schools towards the compliance journey. Lastly, some policy formulations are suggested that would go a long way in ensuring sustainable compliance efforts.

Keywords: *Data protection, sensitive data, privacy, consent, data controller, data processor, processing*.

1.0 Introduction

The twenty-first century is characterized by an increasing reliance on data-driven processes.[2] Personal Data has been termed as 'new oil', and just like crude oil, it must be refined to be useful and valuable[3]. It has also been termed

1 Advocate of the High Court of Kenya, Counsel of the African Court on Human & Peoples' Rights, Accredited Mediator, Business and Human Rights & ESG Consultant & Data Protection Officer.

2 Data Driven Innovation: Big Data for Growth and Well-being (OECD) 2015: Available at: https://www.lisboncouncil.net/wp-content/uploads/2020/08/OECD-Data-Driven-Innovation.pdf. Accessed on 21 July 2025.

3 Title of the speech delivered by British mathematician Clive Humby at a 2006 association of national advertisers' conference: Available at: https://www. https://ico.org.uk/for-the-public/ico-40/data-as-a-commodity/ , Accessed on 20 July 2025

the goldmine for businesses[4]. All sectors of life today, be it in logistics, aviation, agri-business, healthcare, and so on, are using data to predict, drive, and make accurate decisions for both business and Government functions. The education sector is not an exception in this new and fast-accelerating world phenomenon. The need to effectively and efficiently regulate personal data in all its cycle from collection, processing, storage, transmission, sharing, rectification or correction, and deletion in ways that foster privacy and protect human rights cannot be overemphasized.[5] Data protection and privacy in Schools,[6] especially within basic education institutions[7], is not only a statutory compliance requirement, but a safeguarding[8] measure in the form of child protection[9]. Since the enactment of the Data Protection Act[10] and Data Protection Regulations,[11] all schools, regardless of their size, formation or management style, are required by law to register as data controllers and data processors with the Office of the Data Protection Commissioner.[12] To ensure data protection compliance in basic education institutions, the Office of the Data Protection Commissioner

4 Vyautas Kaziukonis linkedin post available on www.linkedin.com/posts/Vyautas -Kaziukonis-today-our-personal-data-is-goldmine-for activity-7206615600494718977-xxxz, Accessed on 20 July 2025

5 Navigating Data Governance: A Guiding Tool for Regulators, available on: https://www.digitalregulation.org/navigating-data-governance-a-guiding-tool-for-regulators/ , Accessed on 20 July 2025.

6 Basic Education Act. No. 14 of 2013, Sec. 2.

7 Ibid.

8 See the Guidance Notes for the Processing of Children Data available on: https://www.odpc.go.ke/wp-content/uploads/2025/05/Draft-1-Guidance-Note-for-Processing-of-Children-Data.pdf; Pg. 18

9 Ibid at Pg. 13.

10 No. 24 of 2019.

11 Published under the Kenya Gazette Supplement No. 236, Legislative Supplement No. 106, available at : https://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2021/LN263_2021.pdf .

12 See the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

(ODPC),[13] as the regulator, has developed guidelines[14] and continues to carry out regular sensitization sessions and technical support to various institutions to assist in their journey to compliance. The regulator flexed its authority and issued enforcement notices to schools to act as a wake-up call. For example, in *Hilda Musimbi Anyama (Suing on behalf of a minor LK) v Friends School Keveye Girls High School*[15]. However, in instances where the ODPC has considered a data breach to be reckless and sensitive, and issued the schools with penalty notices, like in *Christine Wairimu Muturi v. Roma School Uthiru*[16] where the ODPC found the school to have used a minor's photo for marketing without the parent's consent, and in *Everlyn Lavuha Mugita (Suing on behalf of N.S.M – Minor) v Nova Pioneer Kenya Limited*[17] for unlawful processing of a minor's personal data. Whereas enforcement notices[18] are issued in instances where the ODPC considers that the breach may have occurred due to operational lapses and that the school can demonstrate that it is taking all measures to comply and avoid future breaches, penalty notices[19] are issued where a school has not taken any demonstrable efforts and steps to comply with the data protection laws. The ODPC conducts investigations and gives both parties a chance to be heard in writing. The ODPC is then required to render its decision on a

13 Office established under section 5 of the Data Protection Act, 2019. Under section 8, the mandate of the office are as follows: Functions of the Office
(1) The Office shall—
(a) oversee the implementation of and be responsible for the enforcement of this Act.
(b) establish and maintain a register of data controllers and data processors;
(c) exercise oversight on data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;
(d) promote self-regulation among data controllers and data processors;
(e) conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law;
(f) receive and investigate any complaint by any person on infringements of the rights under this Act;
(g) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;
(h) carry out inspections of public and private entities with a view to evaluating the processing of personal data;
(i) promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements;
(j) undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals; and
(k) perform such other functions as may be prescribed by any other law or as necessary for the promotion of object of this Act.

14 See for instance the Guidance Notes for the Education Sector published by the ODPC on 21 March 2024, available at : https://www.odpc.go.ke/office-of-the-data-protection-commissioner-releases-sector-specific-guidance-notes-to-aid-organizational-compliance/ .

15 ODPC Complaint No. 1349 of 2024.

16 ODPC Complaint No. 0841 of 2023.

17 ODPC Complaint No. 1667 of 2024.

18 DPA, Sec. 58.

19 DPA, Sec. 62.

complaint lodged with it within 90 days, as was held in *Gichuhi & 2 others v. Data Protection Commissioner; Mathenge and Others (Interested parties)*.[20] If a party is not satisfied with the decisions of the ODPC, an appeal may be filed in the High Court, and in accordance with its supervisory jurisdiction,[21] it may uphold or overturn the decision of the ODPC.

2.0 Data Protection and Data Privacy

Whereas the two concepts are often used interchangeably, they technically mean two different things. Data privacy refers to an individual's right to control their personal information and decide how much of it is shared with others. It is founded on the fundamental belief that every person should have autonomy to keep aspects of their life private, free from interference or surveillance. It extends beyond just data; it includes personal autonomy, freedom to express oneself, and the ability to maintain confidentiality in various aspects of life, such as personal communication, family matters, etc.

Data Protection, on the other hand refers to legal obligations and measures that must be implemented to safeguard, for instance, student data, staff data, and security data as well as digital records. This is to deter personal data from misuse, loss, or unauthorized access[22].

An example of their distinction in a school set up would be a situation where a fees statement belonging to one parent has been shared with a different parent by the finance office without the consent of the rightful parent. This would amount to a violation of data privacy. However, if the same fees statement is exposed to a third party due to an act of cyber-attack or inadequate security practices in a school, that would be a failure of data protection[23].

The Constitution guarantees the right to privacy of every person[24]. The Data Protection Act, though enacted to give effect to Article 31 of the Constitution, does not use the word 'privacy'. It states its purpose is to make regulations for the processing of personal data, to provide for the rights of data subjects and obligations of data controllers and processors, amongst others[25]. It does not expressly define and distinguish the terms data protection and data privacy.

20 Judicial Review E028 of 2023.
21 Article 165 (1)(c) of the Constitution 2010.
22 Ibid.
23 Ibid.
24 Article 31 (c) and (d).
25 Recital on the objectives of the Data Protection, 2019.

3.0 Schools as Data Controllers and Data Processors

Schools play the dual role of being data controllers[26] and data processors.[27] Schools, therefore, play the data controller role by determining the purpose and means of processing personal data belonging to students, teachers, parents, guardians, visitors, and the non-teaching staff. They hold primary responsibility for ensuring that personal data held by them is processed in compliance with the law and applicable institutional policies. This information is the key data that determines if the school is going to agree to enroll or admit a child to school, or not, depending on the parameters set in the application form for admission and other medical information needed.

Since schools do not largely outsource most of the day-to-day processing activities of personal data collected, they routinely process this data for the provision of educational services. For instance, schools regularly process academic performance data of students across different subjects, skills, and activities by continuously interacting with students' names, images, and their parents' names. They also deal with the processing of sensitive personal data such as medical information, dietary records, and behavioral records.

This twin role of being data controller and processor bestows upon schools the legal obligation to protect children's personal data from the privacy risks of data misuse, unauthorized access, loss, theft, or data manipulation.

4.0 Obligations of Schools as Data Controllers and Processors

Schools as custodians of big data, including sensitive personal data of employees, service providers, and students who are children and who form the bulk of their data subjects, are legally obligated to comply with certain requirements. These mandatory obligations are amongst others the following, (i) to register with the Office of the Data Protection Commissioner as data controllers and or processors[28], (ii) protect and safeguard personal data and ensure processing activities are lawful in accordance with the data protection law[29], (iii) to be transparent about their processing activities and inform the data subjects how their data will be processed or shared[30], (iii) be accountable for the data they are holding[31]. Schools should regularly rectify personal data

26 Means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data; Sec. 2.

27 Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller; Sec. 2.

28 Sec. 18.

29 Sec. 30(3) & 35(2)(b).

30 Sec. 25(b).

31 Sec. 32(4).

which is untrue, inaccurate, incomplete, outdated and misleading following requests from data subjects, (iv) process data portability requests from the data subjects[32], (v) process requests by authorized persons seeking to exercise rights on behalf data subjects[33], and (vi) pay compensation or damages arising from the contravention of the data protection laws[34].

As data controllers and processors, schools must notify the Office of the data protection commissioner within 72 hours of becoming aware of a personal data breach. Where a school is only a data processor, it must also notify the data controller within 48 hours of becoming aware of the administrative breach. Schools should also communicate with concise details of the breach to all the affected data subjects in writing within a reasonable time[35].

5.0 Principles of Data Protection and Privacy

These are the basic frameworks for processing personal data, which is the information relating to an identified or identifiable natural person, the data subject. The main aim of the principles[36] is to (i) harmonize standards for the protection of personal data, (ii) facilitate the accountable processing of personal data for the purposes of implementing the mandates of the data controller and processor, and (iii) ensure respect for the human rights and fundamental freedoms of individuals, particularly the right to privacy.[37] These principles are the following:

A) Lawfulness, fairness, and transparency

This principle has its roots in the openness principle under the OECD Guidelines.[38] This principle stipulates that personal data must be processed in a lawful, fair, and transparent manner.

32 Sec. 38.
33 Sec. 34.
34 Sec. 65.
35 Sec. 43.
36 Sec. 25.
37 Personal Data Protection and Privacy Principles; Adopted by the UN High-Level Committee on Management (HLM) at its 36th meeting on 11 October 2018, available at: https://unsceb.org/sites/default/files/imported-files-UN-Principles-on-personal-data-protection-privacy-2018_o.pdf, accessed on 21 July 2025.
38 The OECD Guidelines for Multinational Enterprises reflect the expectation from governments to businesses on how to act responsibly. They bring together all thematic areas of business responsibility, including human rights and labour rights, as well as information disclosure, environment, bribery and corruption, consumer interests, science and technology, competition, and taxation. This comprehensiveness is a unique feature of the Guidelines and makes it the only government-backed instrument covering all major sustainability risks. Available at: https://www. https://mneguidelines.oecd.org/mneguidelines/ , Accessed on 25 July 2025.

i) Lawfulness – When processing personal data, handlers (data controllers, data processors, third parties, and recipients) must ensure that such dealings with personal data do not breach any applicable law(s), and they must, before such processing, identify the lawful/legal bases upon which they are dealing with the data in the first place[39].

ii) Fairness – This principle is traceable to 1973 in the resolutions of the Council of Europe, which referred to 'fair' collection of data and unfair discrimination[40]. Fairness as a principle of data protection has been noted to lack a precise definition[41]. It is unlike lawfulness, vague, but for processing to be fair, data subjects must be fully aware of processing activities and the entire circumstances surrounding the same[42]. Fairness has also been described as the 'heart' of data protection principles, and its pre-eminence is particularly pronounced by its ubiquity in all data protection laws[43]. The principle has also been described as 'the most fundamental criterion' and 'core principle' of lawful processing of personal data[44].

In the legislative working of the Lindop Report in England in search for its first data protection law in 1978, the report described Fairness Principle thus: *'… the means by which balances are struck and conditions under which the agreements between data subjects and data users are reached are of great importance, where the agreements are voluntary the result will not be fair unless each party fully understands the requirement of the other, and there is clear understanding of what purposes they will be used. Fairness requires openness in such dealings, and it also requires that no advantage should be fallen of any disparities in bargaining power.*'[45]

39 Nicola Fabiano, 'Ethics and Protection of Personal Data' (2019) IMCIC 2019 -International Multi-Conference on Complexity, Informatics and Cybernetics, Orlando Florida, USA, Pgs. 1-17.

40 Resolutions (73) 22 and (74) 2a were adopted to set up systems prohibiting unfair collection and processing of data Council of Europe Convention 108 and Protocols, found at: https://www.coe.int/en/web/data-protection/convention 108/background, accessed on 20 July 2025.

41 Damian Clifford, 'Fairness in Data Protection Regulation-Operationalizing Fairness in Data Protection Officer at Facebook, available at https://hmi.anu.edu.au/ourwork/fairness-and-the-general-data-protection-regulation, accessed on 28 July 2025.

42 Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioral Targeting (PhD thesis, University of Amsterdam, 2014).

43 Daniel-Mahail Sandru, 'The Fairness Principle in Personal Data Processing' (2019) 10(2) Law Review 60, 61.

44 European Data Protection Supervisor, 'Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data (EPDS) (2016) Opinion 8/2016, available at https://www.eaps.europa.eu/sites/default/files/publication/16-09-23_bigdata-opinion_eu.pdf, accessed on 25 July 2025.

45 Norman Lindop, Report of the Committee on Data Protection, (Her Majesty's Stationery Office, 1987) Pg. 11.

In the Google Spain case, for instance, a man complained that Google's continued storage of his personal data relating to his social security debts (which he considered outdated and irrelevant) on the Google search engine was unfair to him, among other claims. The case went to the Court of Justice for the European Union (CJEU), which observed that a fair balance ought to be struck between Google's interest and the data subject's fundamental rights; hence, Google ought to remove the data subject's sensitive information from the webpages, as it was unfair to him. The court specifically held that: *'… the balancing to be carried out…enables account to be taken… of all the circumstances surrounding the data subject's particular situation*.'[46]

iii) Transparency – It has been comprehensively described as *' an act of almost perfect communion between those who decide to process data and the individuals linked to that data during which the latter get to actually see and properly understand what is going on with their data, why this is occurring at all, that will happen to them and their data in the near future and what they could do about it in case they would like to do something about it*'[47]. The objective of transparency as a principle is the provision of information to data subjects on what kind of information about them is collected or dealt with by whom, and the circumstances of such dealings, and any consequences or implications of the same. It requires that data controllers and processors must not only inform data subjects of the collection, use, transmission, sharing, and other activities on their personal data, but they must also ensure that all processing activities on such data are easily accessible and communicated in a manner that can be understood by the data subject [48].

B) Purpose Limitation

This principle effectively assigns data controllers and data processors the duty of ensuring that personal data is only processed for the original purpose of access or collection by mandating controllers and processors to ensure that personal data is not used for incompatible purposes. Its origin is traceable to the earliest conversations around the concept of data protection[49].

46 See Google Spain SL, Google Inc. v AEPD. Case C- 131/12; Casebook on Data Protection (Noetico Repertum, Lagos, 2020) Pg. 490.

47 Gloria Gonzalez Fuster, 'Transparency as Translation in Data Protection; Irina Baralinc Liisa Albertha Wilhelmina Janssens and Mireille Hildebrant (eds) Being Profiled: Logitas Ergo Sum: 10 years of profiling the European citizen (Amsterdam University Press, Amsterdam, 2018).

48 African Journal on Privacy and Data Protection, Volume 1 (2024), Pg. 117, available at: https://www.ajpdp.unilag.edu.ng , accessed on 20 July 2025.

49 Maximilian von Grafenstein, 'The Principle of Purpose Limitation in Data Protection Laws (Nomos

Data controllers and processors must be clear from the outset on what purpose the personal data demanded or processed was meant for, and they must not use such information for other purposes. The reasons for the collection must be unequivocal, and they must not deviate from the same[50]. This principle exhibits two components[51]: (i) purpose specification. This obligates data controllers and processors to collect and strictly utilize data for 'specified, explicit and legitimate purposes disclosed to the data subject (s) at the time of initial collection. The purpose of the collection must be specific and not omnibus. Purpose specification can therefore be broken down to three components: specified purpose, explicit purpose, and a legitimate purpose. (ii) compatible use. The data controller and processor must ascertain compatibility and consider the following: (i) existence of a nexus between original purpose and purpose for further processing, (ii) context of the original collection and reasonable expectation of data subjects based on their relationship with the controller, (iii) consequences of the further processing on data subjects, and (iv) availability of sufficient safeguards[52].

a) Data Minimization

This principle stipulates that the collection of data must be limited to the minimum amount of information necessary to achieve a certain purpose at a given time[53]. This principle contains three requirements that data collected must be adequate for the collection.[54] (i) Data controllers and processors must ensure the suitability, non-excessiveness, and necessity of data collected[55], (ii) the relevant purpose of collection. Only personal data that is patently relatable and valid for disclosed purpose can be collected

Verlagsgeselischaft mbH, Baden-Baden, 2018) Pg. 31.

50 A common example of violation of this principle is found in cases where telephone subscribers' numbers are shared with other organisations for direct marketing purposes. See the case of Emerging Market Telecommunication Service v Eneye (2018) LPELR 46193 (CA) and Godfrey Eneye v MTN Nigeria Communication (Unreported) CA/L/136/2009.

51 Supra Note 48, Pg. 120.

52 Wouter Seinen, Andre Walter and Sari van Grondelle, 'Compatibility Mechanisms for Responsible Further Processing of Personal Data', available at: https://www.bakermckenzie.com/-/media/files/insight/publications/2018/10/compatibility_mechanism_responsible_further_personal_data_processing.pdf?la=en , accessed on 19 July 2025.

53 Meilof Veeningen, Benne de Weger and Nicola Zannone, 'Data Minimization in Communication Protocols: A Formal Analysis Framework and Application to Identity Management' (2014) 13, International Journal of Information Security, Pgs. 529 – 569.

54 Supra Note 48, Pg. 121.

55 Fred H. Cate, 'Failure of Fair Information Practice Principles' in Jane K. Winn (ed) Consumer Protection in the Age of Information Economy, (Ashgate, Farnham, 2006) Pg. 341.

and/or retained by data controllers and processors who must demonstrate the remote or direct nexus between data sought to be processed and the specific purpose disclosed for its processing, (iii) Data controllers and processors are required to interrogate the granular forms of data sets necessary to achieve the organizational goal for such processing activities. Data handlers need to ascertain with exactitude the quantum of data required to achieve specific purposes; hence, where a smaller amount of personal data can be utilized to achieve a certain objective, the utility of a large set of personal data would be adjudged unnecessary[56].

b) Data Accuracy

This principle is described as the 'bulwark' of data protection law[57]. This principle stipulates that controllers and processors that use personal data in the ordinary course of their business operations must ensure that such data accurately reflects the true status of the data subject. The principles obligate data controllers and processors to take appropriate measures to ensure personal data in their custody is accurate and updated. This includes ensuring the completeness, accuracy, and non-misleading nature of the data, and where data is collected directly from the data subjects, to verify the source of such information, to confirm its credibility and currency[58].

c) Storage Limitation

This principle prohibits data controllers and processors from storing data for longer periods than is necessary for the initial purpose of collection[59]. Once personal data has outlived its purpose, it must be deleted or rendered anonymous or pseudonymous. This principle prohibits indiscriminate and unjustifiable accumulation of personal data by controllers and processors, even after they have been put to their original use[60] and to fulfil this obligation, controllers are advised to set justifiable and realistic internal time limits for data

56 Asia J. Biega, Peter Potash, Hal Daume, Fernado Diaz, and Michele Fink, 'Operationalizing the Legal Principle of Data Minimization for Personalization' (2020) SIGIR, Virtual Event, China, 399,400.

57 Dara Hallinan and Fredrick Zuiderveen Borgesius, 'Opinions Can Be Incorrect. (In Our Opinion) On Data Protection Law's Accuracy Principle' (2020) 10 (1) International Data Privacy Law, Pg. 1-2.

58 Eduardo Ustaran (ed), European Data Protection Law and Practice (IAPP, Brussels, 2019) 282.

59 Sec. 39, DPA.

60 See M. Bauer, 'Get Valuable Information From Data Graveyard' (2007), available on https://www.reasearchgate.net/publication/255579707_GET-_VALUABLE_INFORMATION_FROM_THE_DATA_GRAVEYARD, accessed on 202 July 2025.

retention in the absence of a regulatory period.[61]

d) Data Integrity and Confidentiality

This twin principle stipulates that, to guarantee fair processing of personal data, such data must be secured from unauthorized use, alteration, transmission, theft, or corruption. Data controllers and processors are obligated to adopt technical and organizational measures that would secure data from unauthorized or unlawful handling, especially by third parties[62].

e) Data Accountability

This principle obligates data controllers and processors to take all appropriate measures to observe compliance with their obligations under the Data Protection Act. This principle was created to build data subjects' trust in controllers and processors dealing with and handling activities, and serve as a tool to prove compliance with privacy notices[63] displayed by the data controllers and processors. The principle effectively checks the abuse of the processing powers of the controllers and processors who are in control of sensitive information about data subjects. The duty is two-pronged.[64] (i) data controllers and processors are accountable to data subjects on one hand and the supervisory authorities on the other hand, and (ii) to demonstrate fulfilment of this principle, data controllers and processors must periodically report compliance to the authorities, clarify and justify their policies and procedures around their data processing operations.

6.0 Legal and Regulatory Framework

Personal data is regulated nationally, regionally, and globally through the Constitution, laws, conventions, treaties, institutional policies, customs, and an institution's best practices. The following are the legal and subsidiary regulatory frameworks that directly protect and supplement to safeguard

61 Arianna Vedaschi and Valerio Lubello, 'Data Retention and its Implications for the Fundamental Right to Privacy. A European Perspective' (2015) 20 Tilburg Law Review, Pgs 14-34.

62 Supra Note 48, Pg. 124.

63 Cherles Raab, 'The Meaning of Accountability in the Information Privacy Context' in Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener & Hector Postigo (eds) Managing Privacy Through Accountability (Palgrave and Macmillan, London, 2012), Pg. 27.

64 Joseph Alhadeff, Brenda Van Alsenoy and J. Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions in Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener & Hector Postigo (eds) Managing Privacy Through Accountability (Palgrave and Macmillan, London, 2012) Pg. 42.

personal data. They are as follows:

a) The Constitution of Kenya, 2010

The Constitution[65] provides for the right to privacy, which includes the right not to have information relating to one's family or private affairs unnecessarily required or revealed. It also provides for not having the privacy of one's communications infringed upon.

b) Data Protection Act, 2019

This is an Act of Parliament that seeks to operationalize Article 31 (c)and (d) of the Constitution. It established the Office of the Data Protection Commissioner (ODPC).[66] As the institution mandated to protect individual privacy, the provision of rights and remedies for violation of the Act. The law provides a legislative framework for data protection by regulating the processing of personal data, stating the rights of data subjects, and setting out the obligations of data controllers[67] and data processors[68].

c) Access to Information Act, 2016

The Act sets out limitations on right to access to information. It gives effect to the right to access to information of citizens. This information usually contains personal data of individuals from minors to adults.[69]

d) Computer Misuse and Cybercrimes Act, 2018

The Act protects the confidentiality, integrity, and availability of computer systems, programs, and data as well as facilitates the prevention, detection, investigation, prosecution, and punishment of cybercrime.[70]

e) Data Protection Act (Regulations), 2020 & 2021

These are regulations passed pursuant to section 71 of the Data Protection Act. The regulations help in giving full effect to the Act by providing guidelines on general regulations, registration of data controllers, and processors, as well as complaints handling and

65 Article 31 (c) & (d).
66 Supra, Note 12.
67 Supra, Note 26.
68 Supra, Note 27.
69 Sec. 6.
70 Sec. 3 (a) & (d), No. 5 of 2018.

enforcement procedures[71].

f) General Data Protection Regulations (GDPR)

These are the General Data Protection Regulations that apply in Kenya, only to the extent that a data controller and processor in Kenya collect and process personal data belonging to citizens of the European Union. Several schools in the country have students, teachers, and other cadres of employees who are citizens of the European Union[72].

g) African Union Treaty on Cyber Security and Data Protection

Also known as the Malabo Convention, the treaty seeks to address the dangers and risks deriving from the use of electronic data and individual records, with a view to respecting the privacy of the citizens of its member states[73].

h) United Nations Convention on the Rights of the Child[74]

This international treaty provides that no child shall be subjected to arbitrary or unlawful invasion of privacy.

i) The Children's Act, No. 29 of 2022

The Act provides for the privacy of children by prohibiting arbitrary or unlawful interference with their privacy, family affairs, or correspondence. It also provides that the personal data of a child shall only be processed in accordance with the provisions of the Data Protection Act[75].

71 See Data protection (Regulations) General, Registrations of data controllers and data processors & Complaints handling and Enforcement 2021, see also civil registration regulations, 2020 available at: https://www.odpc.go.ke/data-protection-laws-kenya/ ,accessed on 17 July 2025.

72 The General Data Protection Regulations applicable majorly to the European Union which can be accessed at: hhtps://www. https://gdpr.eu/what-is-gdpr/ .

73 The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) was adopted in 2014 at the 23rd AU Assembly of Heads of State and Government to address the regulatory challenges posed by increasing cybercrime on the continent. It also aimed to provide a framework for compatible legislation by member states. Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection .

74 See Article 16 of the United Nations Convention on the Rights of the Child (UNCRC) is a legally binding international agreement setting out the civil, political, economic, social and cultural rights of every child, regardless of their race, religion or abilities adopted on 20 November 1989 by the General Assembly Resolution 44/25. It can be accessed at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child .

75 Sec. 27.

j) ODPC Guidance Notes for the Education Sector

In January 2024, the Office of the Data Protection Commissioner published specific guidance notes for the education sector in accordance with the statutory mandate of developing sector-specific guidelines in consultation with relevant stakeholders. The guidance notes highlight privacy concerns that may arise within the education sector, recommend applying the provisions of the DPA in their day-to-day processing, and provide examples of how the privacy issues may be mitigated or resolved[76].

k) ODPC Guidance Notes on the processing of children's data

The ODPC published draft guidelines for data controllers, processors, and anyone else on how to handle children's personal information and stipulate that children's data needs to be handled with extra caution, ensuring necessary security measures are put in place[77].

l) Policies and Best Practices

Policies serve as a crucial security protocol to systematize the utilization, oversight, and governance of data within an organization. Its paramount purpose is to safeguard and secure every piece of data that an organization handles, stores, or processes, ensuring that it complies with the data protection laws and regulations.

7.0 Consent

Consent in the normal parlance simply means that a person voluntarily and willfully agrees in response to another person's disposition. The person who consents must possess sufficient mental capacity.[78]

Consent is also defined as any freely given, specific, informed, and an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data. The ingredients of Consent are that the consent must be explicit, it must contain an opt-out mechanism that allows parents or guardians

76 'Guidance Notes for the Education Sector'. (ODPC,2023), Available at: https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-for-the-Education-Sector.pdf , accessed on 20 July 2025.

77 Available at: https://www.odpc.go.ke/wp-content/uploads/2025/05/Draft-1-Guidance-Note-for-Processing-of-Children-Data.pdf ,accessed on 25 July 2025.

78 'Consent', see: https://www.law.cornell.edu/wex/consent ,accessed on 17 July 2025.

to withdraw consent at any time and without any consequences.[79]

When obtaining consent, (i) the data controller and processor must ensure that the data subject is informed in a language they understand, (ii) consent is voluntarily given and is specific, and (iii) the data subject has the capacity to understand.[80]

Consent is therefore the ultimate signal that personal data must be dealt with both in strict compliance with the law and the data subjects express wishes. It is conditional in nature where certain conditions must be met, (i) manifestation of express, unequivocal, free, and specific, (ii) informed indication of the data subject's wishes, and (iii) a statement or a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.[81]

In a school setting, consent underscores the importance of safeguarding a child's rights and best interests.[82] The ODDP established guidance notes for consents to guide data controllers and data processors on what the consent should be in line with the principles under section 30 of the Data Protection Act.[83]

8.0 Data Subjects and their Rights

A data subject is an individual whose personal data is collected, held, and processed. A data subject has a right (i) to be informed of the use to which their personal data is to be put, (ii) to access their personal data which is in the custody of a data controller and data processor, (iii) to object to the processing of all or part of their personal data, (iv) to correction of false or misleading data and (v) to deletion of false or misleading data about them.[84]

A data subject may exercise their right where, (i) if the data subject is a minor, by the person who has parental authority or by a guardian, (ii) if the data subject has a mental or other disability, by a person duly authorized to act as their representative, guardian or administrator or, (iv) in any other case, by a person duly authorized by the data subject[85].

79 What does Consent mean? available at: https://www.law.cornell.edu/wex/consent , accessed on 20 July 2025.
80 DPA, Sec. 33.
81 Ibid.
82 Ibid.
83 See Guidance Notes for Consents published by the ODPC available at: https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Notes-on-Consent.pdf ,accessed on 25 July 2025.
84 DAP, Sec. 26.
85 DPA, Sec. 27.

9.0 Data Subjects' Rights in Schools

These can be termed as those rights that automatically attach to an individual whose personal data is collected, held, or processed in whichever form or medium.

A data subject has a right (i) to be informed of the use to which their personal data is to be put, (ii) to access their personal data in custody of data controller and or processor, (iii) to object to the processing of all or part of their personal data, (iv) to correction of false or misleading data about them[86]. Objection to processing personal data is absolutely for direct marketing[87].

The right to be informed must always be done at the point of collecting personal data. The information must be communicated concisely and in plain language. An individual must be informed of the following: (i) how their data will be used, (ii) how long the data will be kept, and (iii) whether their data will be shared with any third parties[88].

Right to correct inaccurate, untrue, outdated, incomplete, or misleading data, where applicable, should be guided by the data subject by furnishing the data controller or processor with documentation that supports their grievance or assertions. These could be documents such as a deed poll of change of name, a marriage certificate, or original documents furnished to the controller or processor, indicating the data is accurate, but for the typographical errors in data entry on their end.

A data subject has a right not to be subjected to a decision based on automated processing, which includes profiling them. This right is only limited by law, where (i) the processing is necessary for the performance of a contract, (ii) is authorized by law, and (iii) is based on consent[89].

A data subject may exercise the above stated rights in a myriad of situations as would probably be in a school, (i) where the data subject is a minor, by a person who has parental authority or by a legal guardian, (ii) where the data subject has a mental or other disability, by a person duly authorized to act as their guardian or administrator or, (iii) in any other case where no minor is involved, by a person duly authorized by the data subject[90].

86 DPA, Sec. 36.
87 Supra, Note 26.
88 DPA, Sec. 26 & 28.
89 DPA, Sec. 35.
90 Supra, Note 84.

In a school ecosystem, the right to data portability is vital. It allows data subjects the right to move, copy, or transfer their data easily from one controller and or processor, in this case, the current school, to the next controller or processor, which is the next school where they are seeking new admission. This right also facilitates reuse of data across different services, such as from one school to another, mainly for enrollment purposes.[91]

Right to deletion or erasure is also commonly referred to as the right to be forgotten and is paramount to a data subject. This right is realistic in that, at some point after leaving school and progressing in one's life, it is just natural that one would be forgotten from their past association, except for other compelling circumstances which are rare and distinguishable from one student or employee to another. This right is mainly exercised if, (i) the data is no longer necessary for the purpose which it was originally collected, (ii) the data subject has withdrawn their consent, (iii) the data subject objects to the processing of their personal data, (iv) processing is unlawful and, (v) there is a legal obligation to delete or erase the data. Of note is that this right does not apply if the processing is necessary, (i) to exercise the right of freedom of expression and information, (ii) to comply with a legal obligation, (iii) for the performance of a task carried out in the public interest, and (iv) for archiving purposes in public interest, scientific research or statistics[92].

Of importance, it is to note that in exercising data subjects' rights on behalf of children, their personal data should not be processed unless (i) the parent or legal guardian is informed, and (ii) explicit consent is always sought where necessary[93].

10.0 Nature of Personal Data Breaches

A personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes[94].

Examples of personal data breaches in a school set up would include but not limited to, (i) access of students, teachers and other employees data by unauthorized party, (ii) deliberate or accidental action or inaction by a controller or processor (school), (iii) sending personal data to incorrect recipients such

91 DPA, Sec. 38.
92 DPA, Sec. 40.
93 DPA, Sec. 33(a).
94 Personal Data Breaches: a guide available at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/ , accessed on 20 July 2025.

as school fees invoices, letters and financial statements, (iv) computing devices containing personal data being lost or stolen, (v) alteration of personal data without permission, and (vi) loss of availability of personal data.

Broadly described, a personal data breach is a security incident that has affected the confidentiality, integrity, or availability of personal data. It means that there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted, or disclosed in a school if someone accesses the data or passes it on without proper authorization, or if the data is made unavailable and this unavailability has a significant negative effect on the data subjects.

11.0 Common Categories of Data Breach in Schools

There are broadly three types of data breaches that can be defined. First, *breach by cause*. These include incidents such as (i) hacking, which is unauthorized access to systems and data through technical means by exploiting software vulnerabilities or causing the installation of malware, (ii) insider threat, which is caused by persons who have legitimate access to the school's data systems of students, parents, guardians, employees, contractors, and visitors. It mainly stems from negligence, malice or ignorance, (iii) physical theft which caused by physical theft or loss of physical devices containing sensitive data such as disks, USB drives, laptops or printed documents or files, (iv) human error which is a result of mistakes made by students, employees, service providers such as misconfiguring databases, sending information to the wrong recipients or improper disposal of records, and (v) social engineering which is caused by manipulating individuals into disclosing sensitive information through tactics like pre-texting or baiting.[95]

Second, *breach by the kind of data compromised*. This is the category of the specific data that the attacker was able to access, depending on whether it was sensitive or not. Exposure of data requires different kinds of responses due to the inherent consequences each breach poses to a school. This category would include, (i) personal identifiable information which is data can be able to identify an individual, such as names, addresses, NHIF number, personal car number plates, date of birth, NSSF number etc., (ii) financial information which includes bank account details, credit card number and payment information etc., (iii) health information which includes medical records, health insurance information and any other data classified as sensitive personal data, (iv) login credentials such as usernames, passwords and authentication

95 Waya to categorize types of data breaches available at: https://www.docontrol.io/blog/the-3-types-of-data-breaches-and-their-dangerous-impact-on-your-data ,accessed on 25 July 2025.

details.[96]

Third, *breach by impact on data*. This kind of breach looks at the overall impact of what the breach did on the data. It is categorized into three (i) confidentiality breaches, which is when sensitive data is exposed to unauthorized persons. It may also manifest as an intentional confidentiality breach when large volumes of data are copied and removed from a school's system, and when specific targeted data is, such as students' or employees' information, is stolen, (ii) integrity breach, which is the unauthorized alteration or destruction of data. It manifests when data assets are altered without authorization, impacting their accuracy and reliability, when false data is injected into a school system, and when data is simply removed from a school system, (iii) availability breach, which is the disruption to the school's access or use of its data or information. Intentional availability breach may manifest when a data service is overwhelmed by illegitimate requests to the system, disrupting access for legitimate users. It may also manifest when malware encrypts data, making it unusable and inaccessible to the school, and demands for ransom payment for decryption are made.[97]

12.0 Ways in Which Data Breach Could Occur in School Databases

These are the possible attacks that could occur and result in a massive breach of data and privacy. The list is not exhaustive, but a highlight of selected common attacks on school systems. They are, (i) stolen information where a student or employee has left a computer or even physical files unsecured, (ii) ransomware which involves getting an email stating that your computer is now encrypted denying one access to their data for extortion purposes, (iii) password guessing which happens when attackers notice that students or employees leave their passwords on post it notes allowing anyone to access them, (iv) recording keystrokes happens when cyber criminals insert or send an email containing malware that if one clicks on it can cause the criminal to record what one is typing on their computer, (v) malware or virus sent to persons to wipe their computer of all the data in their systems, and (vi) distributed denial-of-service when an attack is launched from multiple sources simultaneously[98].

96 Ibid.

97 Ibid.

98 The most common types of data breaches and how they affect your business available at: https://www.veritas.com/information-center-most-common-types-of-data-breaches-and-how-they-affect-your-business ,accessed on 25 July 2025.

13.0 Data Mapping as a Strategic Measure for Schools

Data mapping is a strategic discipline that underpins operational integrity, risk management, and demonstrable accountability. At its core, data mapping captures and visualizes the journey of personal data through the entire school ecosystem. It shows where data is collected, how it is processed, who has access to it, where it is stored, how it is shared, and ultimately how it is deleted or erased. Data mapping is simply a legal infrastructure that offers clarity, control, and confidence in how a school handles personal data throughout its lifecycle[99].

It is a requirement of the law for a school to either employ or designate a suitable person well-trained and versed with the data protection law as its Data Protection Officer (DPO). The DPO is crucial for assisting the school in translating regulatory requirements into practical operational applications. Data mapping gives the DPO direct oversight of how personal data is handled across the school(s). It sharpens the staff and empowers them to be able to assess legal risks, respond to incidents, advise on technology adoption, and demonstrate compliance to the ODPC as the regulator with more efficiency, speed, and confidence.[100]

Data mapping is a strategic tool that, if done correctly, would assist a school in achieving a couple of milestones in the compliance journey. These are (i) legal accountability under the Data Protection Act. Without a complete understanding of data processing, schools risk breaching the Data Protection Law. A school should develop a Record of Processing Activities (ROPA) as a regulatory artefact, as the real foundation for an accurate and up-to-date data map. It provides the DPO with the narrative needed to demonstrate the school's awareness, control, and readiness. (ii) Fast, defensible data subjects' access requests. A well-maintained data map transforms what could be a scavenger hunt into a controlled and auditable process. DPO can isolate systems, pull targeted datasets, and document compliance to ensure adherence to regulations. (iii) risk management in real time. From vendor due diligence to breach response, data mapping equips the DPO with the context required to move quickly. It supports internal investigations; shapes incident reports, and clarifies which jurisdictions or categories of data subjects are affected, especially for schools with multicultural diversity. This is critical information for determining notification obligations[101].

99 Sacha Kirk, 'Data Mapping: Essential Insights Every DPO And In-House Team Needs To Know' available at: https://www.lexology.com/library/detail.aspx?g=0435cce5-8c59-4240-bf9f-c64776144a58 ,accessed on 20 July 2025.

100 Ibid.

101 Ibid.

Data mapping can be embedded into the school operations in different ways, such as (i) running a targeted data audit. This is achieved by partnering with other departments to catalogue data processing activities. It helps in documenting not only what data is collected, but also why and under which lawful basis it is being sought. (ii) maintain dynamic flow maps. This is achieved by translating audit findings into visual diagrams that show real movement. The diagrams support legal reviews, impact assessments, and internal governance. (iii) Linking with the Record of Processing Activities (ROPA). ROPA must echo or align with the structure of the school's data map. It is useful as a reference point in vendor assessments, internal policies, and Data Protection Impact Assessments (DPIAs). (iv) scrutinize vendor data practices. Each processor relationship should be mapped. This is what data they collect, where it is stored, and what breach terms are in place. (v) enrich privacy impact assessments. Data mapping feeds Data Protection Impact Assessments with real operational insights. This makes Privacy Impact Assessments shift from being mere hypothetical to practical, with specific risks and mitigations to conform with the school operations. (vi) training tool. The data map is an essential training asset. The DPO should regularly train employees and illustrate to them how their school operations and processes fit in with the broader data landscape. Staff training and regular sensitization foster ownership and help identify issues early.[102]

Whilst data mapping is essential for Data Protection compliance, its real value is in the broader operational and strategic benefits it brings on board. For the DPO and key staff managing risk, enrollment, contracts, employment, and appointments, data governance, and regulatory relationships, the pros extend well beyond audit readiness. Data mapping is crucial for (i) legal risk management. A well-structured data map reveals where the school is or may be exposed. This could be, for instance, outdated enrollment or admission forms, which are the substantive contracts between the school and the parents or guardians. The DPO is equipped with the essential insights for prioritizing remediation efforts and can target legal reviews where the most impact would be. (ii) contractual clarity and control. Data mapping highlights which third parties access personal data and under what legal basis. This helps the school staff involved or the DPO to assess whether service level contracts contain appropriate data protection safeguard clauses and adequate indemnity provisions. (iii) efficient breach response. Time is of the essence when it comes to a personal data breach. With the mandatory statutory timelines for reporting a data breach, a real-time data map enables the DPO to quickly understand which categories of data were affected, which jurisdictions are in

102 Ibid.

scope, and whether the incident triggers reporting obligations, allowing for quicker appropriate action. (iv) due diligence. In any dealings, data subjects are increasingly scrutinizing how their personal data is being handled[103].

14.0 Policies to guide in compliance

According to the Oxford English Dictionary, a 'policy' refers to a definite cause or method of action selected from alternatives to guide and determine present and future decisions. Schools as big data handlers (data controllers and processors) should consider formulating effective and adequate policies as suggested below.

a) *Data Protection and Privacy Policy*. This is a policy that signifies the strategic and procedural steps undertaken to safeguard the privacy, availability, and integrity of sensitive personal data[104].

b) *Data Subjects Rights Handling policy*. This policy would outline the procedures for handling requests from data subjects who wish to exercise their rights, such as access, rectification, erasure, objection, and data portability. It ensures timely responses to such requests[105].

c) *Personal Data Breach Incident policy*. This is a structured plan that details the steps to be taken in the event of a data breach. It includes procedures for identifying, containing, assessing, and mitigating, and reporting breaches to the ODPC and the affected individuals. The policy ensures a quick response in compliance with statutory notification requirements[106].

d) *Data Retention and Disposal Policy*. The policy specifies how long different categories of personal data should be retained and the secure methods for disposing of data that are no longer needed. It ensures personal data is retained only for as long as necessary for its intended purpose. It also outlines secure disposal mechanisms to prevent unauthorized access or misuse of personal data[107].

103 Ibid.

104 What is Data Protection and Privacy available at: https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/ ,accessed on 26 July 2025.

105 See Anne Babu & Co. LinkedIn page available at: https://www.linkedin.com/posts/anne-babu-co_labourlaw-kenya-kenyaemploymentlaw-activity-7313794983151460352-askh?utm_source=share&utm_medium=member_android&rcm=ACoAABwQ2zUBTxWBLshNK3yTLhQUV7PKKmG8Yt8 , accessed on 28 July 2025.

106 Ibid.

107 Ibid.

e) *Information Security/ IT policies*. This policy establishes the technical and organizational measures necessary to protect personal data from unauthorized access, alteration, and disclosure, or destruction. The policy covers areas such as access control, encryption, cybersecurity protocols, secure authentication methods, and regular security audits[108].

f) *Safeguarding policy*. This is a comprehensive policy designed to ensure the safety of young people, which protects them from abuse[109].

15.0 Conclusion

Data protection and privacy compliance have increasingly become the new day-to-day requirement for every school in the country. Private schools have particularly been hard hit by this mandatory statutory compliance requirement, which has sent shockwaves across the sector after several private schools were heavily fined and penalized by the ODPC for various personal data breach violations. Several other private schools, for instance, have been served with enforcement notices which have further demonstrated that all schools are at the ODPC's arm's length.

This mandatory statutory compliance requirement has caused several schools to create urgent budgetary allocations for either training and retooling of their existing staff to take up the Data Protection Officer's (DPO) role, or recruiting professionally trained DPOs externally.

Compliance with data protection and privacy is a trend that will have no end in sight. It will continue to perpetuity, especially in this era of mass social media, artificial intelligence, cybersecurity, cyberthreats and intelligence gathering. Compliance will therefore require consistent and constant data impact assessments, training, and review of policies and procedures, and operating procedures in every school. Personal data protection and privacy compliance will not be an event, but a long journey ahead that will be passed from one generation of school management to the next.

108 Ibid.

109 See for instance , 'What is Safeguarding in Schools available at: https://www.supportingeducation.com/content-hub/safeguarding-in-schools-importance-and-strategies/, accessed on 28 July 2025.

LAW SOCIETY OF KENYA

To advertise here, please contact the Law Society of Kenya through lsk@lsk.or.ke or call 0799- 595 800

Public Participation in Kenya: Balancing the Authority of the Electorate and the Elected

Wahome Wilson[1]*

Abstract

This article examines the intricate balance between representative decision-making and direct citizen engagement in Kenya's legislative process. It interrogates the extent to which elected Members of Parliament, entrusted with advancing the public interest, may legitimately exercise independent judgment even when it diverges from the expressed will of their constituents. Drawing from Kenya's constitutional provisions on sovereignty and public participation, the discussion situates the debate within the broader context of participatory democracy and representative governance. The article samples relevant judicial interpretations that have shaped the understanding of public participation and its binding effect on legislative outcomes. It also considers the tension between parliamentary autonomy and the constitutional imperative to uphold the people's voice as the ultimate source of authority. By assessing both theoretical perspectives and practical experiences from recent legislative processes, the article seeks to address whether the electorate's voice should hold absolute primacy or if representatives possess the discretionary authority to act contrary to public opinion for the perceived greater good. In doing so, the article contributes to ongoing discourse on democratic accountability, constitutionalism, and the evolving relationship between citizens and their elected representatives in Kenya's governance landscape.

Keywords: *Public participation, Constitutional democracy, Popular sovereignty, Representative governance, Parliamentarians, Electorate*

1.0 Introduction

Public participation has many, albeit related, definitions and purposes. It may refer to a process where stakeholders are involved directly or indirectly in decision-making about policies, plans, and programs that they have an interest in.[2] Callon et al define it as a broad set of activities and situations

1 *Wilson Wahome is a legal consultant and researcher specializing in technology law, intellectual property, data protection, and privacy. He is the founder of GW Rifa Consulting that focuses on advising multinationals, startups, civil society organizations, and public institutions. His work also focuses on governance, digital rights, regulatory compliance, and the intersection between law, technology, and public policy.

2 Kathryn S Quick and John M Bryson, 'Public Participation' in *Handbook on Theories of Governance* (Edward Elgar 2022) 656 https://doi.org/10.4337/9781800371972.00022 accessed 15 October 2024.

that may or may not be spontaneous, organized, and structured, where non-experts provide their input regarding policies and their formation.[3] Kenya's Draft Policy on Public Participation of 2018 offers the following definition of public participation, "the process by which citizens, as individuals, groups or communities (also known as stakeholders), take part in the conduct of public affairs, interact with the state and other non-state actors to influence decisions, policies, programs, legislation and provide oversight in service delivery, development and other matters concerning their governance and public interest, either directly or through freely chosen representatives."[4] Bobbia provides a broader definition of public participation. He argues that it (public participation) is a tool through which policymakers outsource some policy design elements to citizens. He further asserts that participation is not limited to a particular group. It may be done by those who are economically empowered and those who are not, it may be done physically or digitally, for short or long periods, and may be regarding important or 'trivial' matters.[5] Kenya's Constitution, promulgated in 2010, does not define the term public participation. It, however, mandates that any business transacted by Parliament should be conducted openly and transparently. Under Article 118 (1) (b), the Constitution requires Parliament to facilitate public participation and involvement in any business that it conducts, including but not limited to its law-making function. However, this is not the only reference to public participation in the Constitution, as the concept is also enshrined in articles 10(2)(a) and 232(1)(d) as one of the values and principles of governance.

Public participation is, therefore, a critical tenet of the legislative process that lawmakers cannot bypass. The Constitution speaks not just of public participation, but involvement. The two are subtly different, but this difference is critical to understanding how the law-making process works. To participate is to take part; to have a part or share *with* a person, *in* a thing; to share.[6] In this way, participation may be viewed as a process that allows stakeholders, including citizens, to take part in, by contributing to, the creation of laws used to govern them. Involvement, on the other hand, means to include someone or something in an activity.[7] Involvement appears to be deeper and less superficial or procedural than participation. Hence, the process should be one that not

3 Michel Callon, Pierre Lascoumes and Yannick Barthe, *Agir dans un monde incertain: Essai sur la démocratie technique* (Éditions du Seuil 2001) 16.

4 Office of the Attorney General and Department of Justice, *Kenya Draft Policy on Public Participation* (2018).

5 Luigi Bobbio, 'Designing Effective Public Participation' (2019) 38(1) *Policy and Society* 41 https://doi.org/10.1080/14494035.2018.1511193 accessed 16 October 2024.

6 *Oxford English Dictionary* (2nd edn, 1989) sv 'Participation'

7 *Cambridge Dictionary* (4th edn, 2013) sv 'Involve'.

only collects the views of the public and stakeholders but also considers and incorporates them carefully and seriously when creating laws.

2.0 A Flurry of Laws: The Constitutional Right to Public Participation

There has been a notable surge in the revenue-raising measures in Kenya, more particularly after the Kenya Kwanza alliance took the reins of power, and this has involved passing controversial laws in a bid to raise taxes.[8] The country's debt situation has been worsening year on year, and raising taxes to pay off the mounting debt that now stands at 70% of GDP[9] was seen as the only sure way to dig the nation out of the hole it currently finds itself in. The flurry of laws has been met with resistance at numerous points, most significantly in 2024 when the proposed Finance Bill was widely criticized, sparking protests in many parts of the country, and was eventually dropped.[10] The protests were the clearest manifestation of public participation. There was a clear disconnect between legislators and constituents as parliamentarians forced the Bill through despite overwhelming opposition from the people.

The insistence by Parliamentarians to exclude and/or ignore the public's voice from the lawmaking process means that courts regularly have to be called upon to intervene and help exercise the populace's ultimate power. Public participation has brought down several laws that have glossed over the process or treated it as a mere formality. The most prominent casualties have been the Finance Act, 2023 (ultimately revived by the Supreme Court of Kenya), the Constitution of Kenya (Amendment) Bill, 2020, the Social Health Insurance Act, 2023, and the Privatization Act, 2023. The Constitution of Kenya has ensured that ultimate power rests with the people and that such power may be exercised directly or indirectly. [11] It therefore follows that the people who wield this power must be involved in the debate and design of decisions that affect any part of their lives and their future. Their power does not begin and end at the ballot box; instead, it remains with the people continuously, ready to be exercised or reclaimed at any moment.

This tension between the public and lawmakers raises a fundamental question: ***Whose voice should be prioritized when making the laws that govern***

8 John Mutua, 'Is Kenya Kwanza Administration's Push for Higher Taxes Misguided or a Masterstroke?' (IEA Kenya Blog, 7 November 2023) https://ieakenya.or.ke/blog/is-kenya-kwanza-administrations-push-for-higher-taxes-misguided-or-a-masterstroke/ accessed 15 October 2024.

9 Cytonn, 'Review of Kenya's Public Debt 2024' https://cytonn.com/topicals/review-of-kenyas accessed 29 October 2024.

10 Gustav Gilund, 'Krever kraftige endringer' *Klassekampen* (17 July 2024) https://klassekampen.no/artikkel/2024-07-18/krever-kraftige-endringer accessed 16 October 2024.

11 *Constitution of Kenya* art.1

society? Should it be the elected representatives whose mandate is to act in the best interest of the people (and who have been entrusted with such power by the people), or the constituents themselves, who bear the direct impact of these laws and policies? This question is at the heart of democratic governance and begs for an in-depth analysis of whether representatives are truly bound by the will of the electorate or are entrusted with the discretion to act independently in what they deem to be the public's best interest.

3.0 The Role of Parliamentarians

Parliament functions through the fulfillment of three distinct yet interrelated roles: legislative or lawmaking, oversight, and representative responsibilities.[12] The legislative function includes making laws, regulations, and policies that govern the people. In addition to creating new laws, parliament is also tasked with amending, approving, or rejecting any laws that come from outside the House.[13] Johnson (2005) also argues that the lawmaking function of parliament does not exist in a vacuum. For lawmaking to be effective, differences in society must be represented, and members must compromise on some elements and agree on others to have a holistic final output.[14] The difficulty of making laws that appeal to all members of society is perhaps best expressed in the Preliminary Report by the Inter-Parliamentary Union,

> *"As the elected body that represents society in all its diversity, parliaments have a unique responsibility for reconciling the conflicting interests and expectations of different groups and communities through the democratic means of dialogue and compromise."*[15]

This difficulty is further compounded by the need to consider the general will of the people as put forth in Jean Jacques Rousseau's *The Social Contract.* [16]

In addition to establishing laws and policies that govern the people, legislature oversees the actions of the executive and ensures that the laws passed in the House are properly implemented. This "checks and balances" function is not just confined to reviewing the implementation of laws but also extends to spending by the government. This function is critical as it establishes parliament's role

12 John K Johnson, 'The Role of Parliament in Government' (World Bank Institute Working Paper 2005) 2

13 Ibid 3

14 Ibid 3

15 Inter-Parliamentary Union, *Parliament and Democracy in the 21st Century* (2005) http://archive.ipu.org/splz-e/sp-conf05/democracy-rpt.pdf.

16 Christopher Bertram, 'Jean Jacques Rousseau' in *The Stanford Encyclopedia of Philosophy* (Summer 2024 edn, Edward N Zalta and Uri Nodelman eds, 21 April 2023) https://plato.stanford.edu/archives/sum2024/entries/rousseau accessed 2 November 2024.

as a defender of the citizens' rights. [17] It is also the most difficult due to several factors. The first is that political alignment and partisanship often hinders effective scrutiny, as parliamentarians may prioritize party loyalty over holding the executive accountable. Secondly, dissident members may be whipped into submission through a series of actions and sanctions, including expulsion from the party and withdrawal of support in future elections.[18] In instances where members belong to the ruling party, checks on government power may be severely compromised or become entirely nonexistent. Additionally, many parliaments face resource and capacity constraints, lacking the technical expertise, staff, and access to relevant data necessary for thorough investigations.[19] In systems where the executive holds significant power, parliamentary oversight is further constrained as individuals may resist scrutiny or delay responses.[20] Conflict of interest and corruption also undermine oversight, with parliamentarians potentially benefiting from their relationships with the executive, weakening their incentive to investigate wrongdoing. Institutional weaknesses, such as a lack of enforcement mechanisms, further complicate oversight, as parliamentary committees or oversight bodies may only have the power to recommend changes without the ability to enforce them.[21] Together, these factors create significant obstacles to effective parliamentary oversight, which is essential for democratic accountability.

The third role of parliament is representation. The first two functions of lawmaking and oversight are exercised by parliament in its representative capacity.[22] Although Jean Jacques Rousseau argues that vesting legislative or oversight authority in an individual or a group of people is tantamount to slavery and a symptom of moral decline and loss of virtue, the difficulty of direct self-rule by citizens is obvious.[23] First, scale is a major issue. In large, heterogeneous countries with millions of citizens, it is logistically impossible to gather everyone for collective decision-making, making direct democracy unfeasible beyond small, localized communities.[24] Additionally, the complexity

17 αgora, 'Parliamentary Function of Oversight' (Portal for Parliamentary Development) https://www.agora-parl.org/resources/aoe/parliamentary-function-oversight accessed 20 October 2024.

18 David Beetham, *Parliament and Democracy in the Twenty-First Century: A Guide to Good Practice* (Inter-Parliamentary Union 2006) 40.

19 Beetham (n17) 41.

20 Hironori Yamamoto, *Tools for Parliamentary Oversight: A Comparative Study of 88 National Parliaments* (Inter-Parliamentary Union 2007) 11.

21 Pascal B Mihiyo, Truphena E Mukuna and Herman Mushara, 'Needed: A Legal Framework for Strengthening Oversight Roof of the Kenyan Parliament' (OSSREA Policy Brief, Addis Ababa 2016) 2.

22 αgora, 'Parliamentary Function of Representation' (Portal for Parliamentary Development) https://www.agora-parl.org/resources/aoe/parliamentary-function-representation accessed 20 October 2024.

23 Betram (n17) para 32.

24 Meta Mendel-Reyes, 'Self-Rule or Selves-Rule? A Problem in Democratic Theory and Practice' (1999) 32(1) *Polity* 28 https://doi.org/10.2307/3235332 accessed 31 October 2024.

of issues further complicates direct self-rule, as most contemporary policy decisions—such as those concerning economic regulation, foreign policy, and technological governance—require specialized knowledge that the average citizen may not possess. This creates a knowledge gap between citizens and policymakers. Time constraints also pose a significant barrier, as the demands of daily life leave little room for most citizens to engage in continuous deliberation and decision-making. Direct self-rule would require citizens to dedicate substantial amounts of time to governance, which is impractical for most. Finally, the risk of majority tyranny looms large in direct self-rule, where the will of the majority might consistently override the rights and needs of minorities, leading to injustices that representative systems aim to mitigate through checks and balances.[25]

Carrying out these functions effectively contributes to democracy.

4.0 Representation versus Usurpation? Parliament's Duty to Represent the Electorate

Effective representation, one of the core functions of Parliament, is both complex and multilayered. As previously highlighted, party alignment and loyalty often play a significant role when lawmakers are called upon to make decisions regarding new or existing policies. This creates a balancing act where representatives must navigate the expectations of their party or party leader while considering the needs and demands of their constituents. Complicating the decision-making even further is the knowledge gap that frequently exists between policymakers and the electorate. Parliamentarians are often tasked with making decisions that involve intricate economic, legal, or social considerations, which may be difficult for the public to fully grasp. These decisions may lead to short-term pains but promise long-term benefits. However, if the electorate's understanding of proposed laws is limited and focuses solely on the immediate negative effects—such as economic burden or reduced freedoms—they may resist such policies, despite their potential for future gains. This has been the song sung by many politicians in Kenya who argue that citizens should tighten their belts now, with the promise of loosening them in a few years. This dissonance between the short-term concerns of the electorate and the broader, long-term objectives of lawmakers poses a fundamental challenge to representative democracy, as it can foster frustration, misunderstanding, and even distrust in the legislative process. The only way to bridge this gap is through greater efforts in civic education and engagement. This will ensure that the electorate is not only consulted but also adequately informed and understands the bigger picture regarding any proposed policy.

25 Ibid 29.

With all the challenges inherent in representative democracy, the key question emerges: "Who comes first, the parliamentarian or the constituent?" To address this, we must examine two key models of representation - the trustee model and the delegate model. The trustee model is perhaps best articulated by Edmund Burke in his famous speech to his Bristol electorate. Burke stated,

> *"My worthy colleague says, his will ought to be subservient to yours. If that's all, the thing is innocent. If government were a matter of will upon any side, yours, without question, ought to be superior. But government and legislation are matters of reason and judgment, and not of inclination; and what sort of reason is that, in which the determination precedes the discussion; in which one set of men deliberate, and another decide; and where those who form the conclusion are perhaps three hundred miles distant from those who hear the arguments?"*[26]

Burke argued that governance and representation should be guided by reason and informed discussion, rather than the immediate desires of constituents. The trustee model of representation is premised on the idea that elected representatives can and should make decisions that are in the best interests of their constituents as opposed to subjecting themselves entirely to their will.[27] Burke went further to state to his electorate that,

> *"You choose a member indeed; but when you have chosen him, he is not a member of Bristol, but he is a member of Parliament."*

His message was clear. While a representative must consider the needs and interests of their constituents, they must also be free to exercise independent judgment and thought guided by the broader good and long-term vision, even if it means occasionally opposing the will of the electorate.

The delegate model has been less controversial among democracies and citizens. McCrone and Kuklinski (1993) define it as a mode of representation where legislators are required to reflect and prioritize the preferences of their constituents.[28] For many, the member of parliament is seen as only being a representative who is a stand-in for the constituents. He does not and should not have independence of thought or judgment. Pitkin (1967) says of representatives,[29]

> *"A mandate theorist will see the representative as a "mere" agent, a servant, a*

26 Edmund Burke, *Speech to the Electors of Bristol* (3 November 1774).

27 Mateusz Brodowicz, 'The Trustee Model of Representation Explained' (Aithor) https://aithor.com/essay-examples/the-trustee-model-of-representation-explained accessed 1 November 2024.

28 Donald J McCrone and James H Kuklinski, 'The Delegate Theory of Representation' (1979) 23(2) *American Journal of Political Science* 278 https://doi.org/10.2307/211103 accessed 1 November 2024.

29 Hanna Fenichel Pitkin, *The Concept of Representation* (University of California Press 1967) 146.

> *delegate, a subordinate substitute for those who sent him. The representative, he will say, is "sent as a servant" not "chosen with dictatorial powers," and so the purpose which sent him must have been the constituents' purpose and not his own. They sent him to do something for them which they might have chosen to do for themselves, which they are perfectly capable of doing and understanding…"*

In the delegate mode of representation, lawmakers and representatives ought to mirror the preferences of their constituents. This approach emphasizes the idea that ultimate authority rests with the electorate, with representatives acting as faithful executors of the public's wishes.

5.0 Conclusion

The legislative process and the affairs of a country that need the input of parliamentarians seem to be at loggerheads. On the one hand, lawmakers should have the freedom and independence to make sound decisions on behalf of the electorate. On the other hand, however, these lawmakers are stand-ins for the electorate and should act as directed by the people.

Parliamentary decision-making should be grounded in the rule of law and aligned with the interests of society. However, a persistent impasse often arises between parliamentary agendas and public opinion due to deviations from these core principles. In Kenya, for instance, concerns have frequently surfaced about the quality of laws enacted by both the national and county governments.[30] Many of these laws have faced legal challenges in court, questioning their constitutionality and legitimacy.[31] This disconnect highlights a gap between policymakers and the electorate, who increasingly feel that their voices are disregarded in the face of apparent indifference from lawmakers. Certain legislators have even publicly asserted that laws will pass as drafted, irrespective of public opinion, suggesting a lack of empathy, sincerity, and openness to citizen input—an attitude that many interpret as indicative of self-serving motives.[32]

If these laws were truly crafted for the public good rather than for self-interest, Parliament would prioritize civic education to foster public understanding and build support, ensuring alignment with the citizenry. The fact that some of

30 Rose Oronje, 'Challenges with Evidence Use in Kenya's Legislative Process' (AFIDEP, 2 November 2024) https://afidep.org/challenges-evidence-use-kenyas-legislative-spaces/ accessed 2 November 2024.

31 Kamau Muthoni and others, 'Blot on Parliament as MPs Churn Out Bad Laws' *The Standard* https://www.standardmedia.co.ke/article/2000190565/blot-on-parliament-as-mps-churn-out-bad-laws accessed 3 November 2024.

32 Fredrick Ooko, 'We Will Pass the Finance Bill, Gov't Does Not Lose – MP Sylvanus Osoro Says' *Citizen Digital* https://www.citizen.digital/news/we-will-pass-the-finance-bill-govt-does-not-lose-mp-sylvanus-osoro-says-n319621 accessed 3 November 2024.

these laws have been struck down for failing to meet constitutional standards suggests that Parliament sometimes advances poorly conceived legislation. It is this departure from the rule of law that creates friction between lawmakers and the citizens. The result is a severe loss of trust and a widening of the gap between government and the people it serves.

Article 1 of Kenya's Constitution reads,

1. (1) All sovereign power belongs to the people of Kenya and shall be exercised only in accordance with this Constitution.

(2) The people may exercise their sovereign power either directly or through their democratically elected representatives.

The Constitution vests ultimate power in the people and gives them the liberty to exercise their power either directly or indirectly. The same Constitution also recognizes that Parliament has a critical role to play in the country through its mandates of oversight, lawmaking, and representation. The question of whose opinion takes precedence in matters of law and policymaking is however, not envisioned. The ongoing tension between lawmakers and citizens in matters requiring the public's input highlights a fundamental challenge in democratic governance: aligning legislative intentions with the will of the people. The greater challenge for Kenya or any other nation is the self-interests of the lawmakers.

"We got a Constitution in 2010. We didn't get constitutionalism."[33]

As highlighted, when laws are understood as only serving narrow interests or lack a basis in the rule of law, citizens feel alienated, and the legitimacy of Parliament's decisions comes into question. To bridge this gap, lawmakers must prioritize transparency, genuine public engagement, and a commitment to constitutional values. Ensuring that legislation reflects both the common good and public opinion not only strengthens trust in the legislative process but also promotes laws that are sustainable and respected. Ultimately, the country will only grow when both Parliament and the citizenry work collaboratively toward shared goals, each recognizing the value of the other's voice in shaping the laws that govern all.

33 John-Allan Namu, 'Maoni' (X, 9 July 2025) Video https://x.com/johnallannamu/status/1942938442570301750 accessed 10 November 2024.

THE LAW SOCIETY OF KENYA
JOURNAL

Lavington, Opposite Valley Arcade, Gitanga Road
P.O Box 72219-00200 Nairobi
Tel: +254 799 595 800
lsk@lsk.or.ke, www.lsk.or.ke