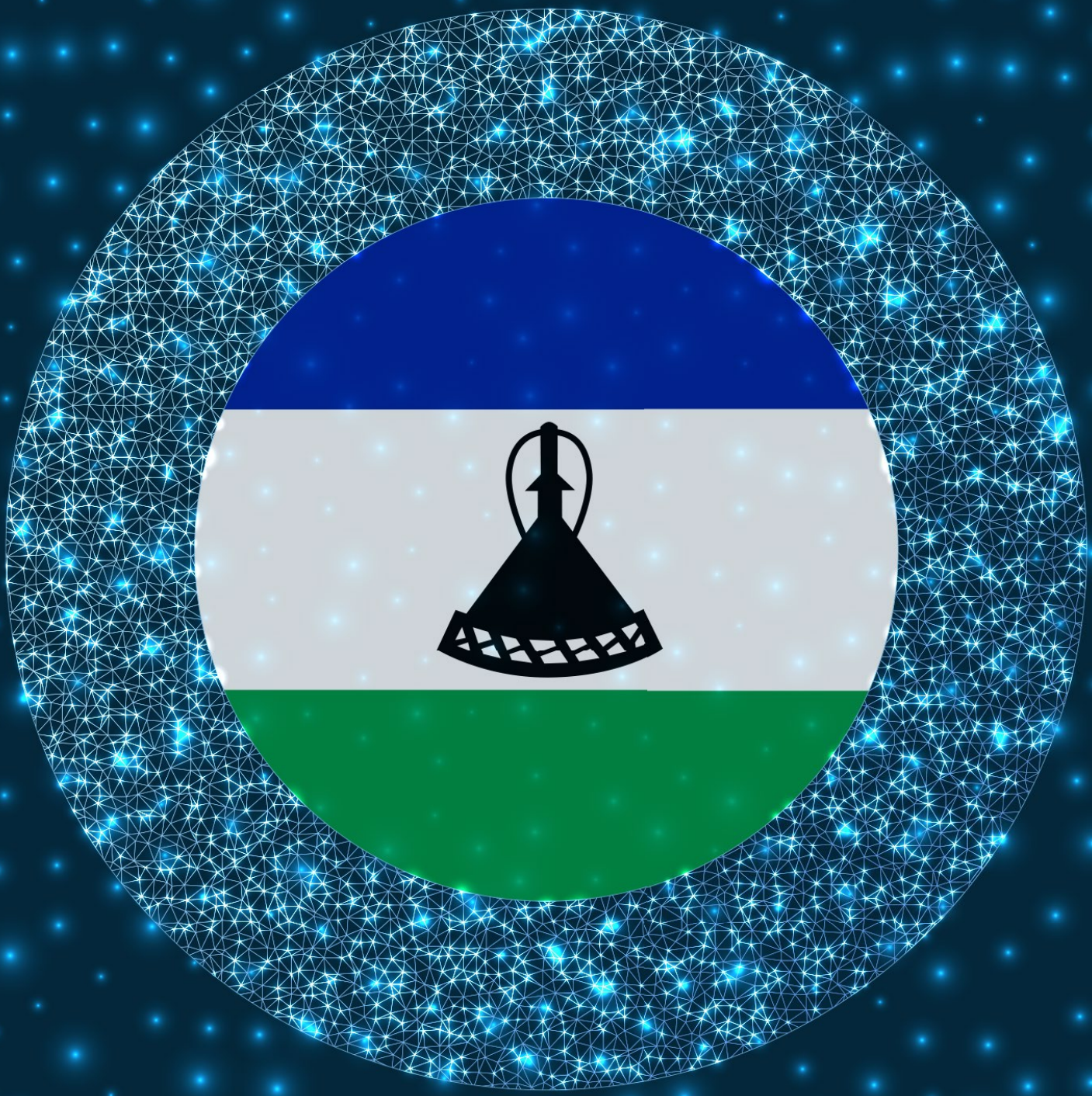


Digital Rights in Lesotho:
A Situational Analysis


UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA


Centre for
Human Rights
UNIVERSITY OF PRETORIA


ADVANCING RIGHTS
IN SOUTHERN AFRICA
ARISA


Transformation
Resource Centre


Internews
Local voices. Global change.

TABLE OF CONTENTS

ISBN: 978-1-7764485-8-6

Author: Dr Matšepo Regina Kulehile

Editors and Reviewers: Hlengiwe Dube, Ompha Tshamano, Marystella Auma Simiyu and Mokitimi Tšosane

Acknowledgements:

The research work was commissioned by the Centre for Human Rights, Faculty of Law, University of Pretoria (the Centre). This report was researched and written by Dr Matšepo Regina Kulehile from the National University of Lesotho, while the review and editorial processes were undertaken by Hlengiwe Dube, Ompha Tshamano and Marystella Auma Simiyu of the Centre for Human Rights as well as Mokitimi Tšosane of the Tranformation Resource Centre who assisted with the review. The Centre expresses its gratitude to the Transformation Resource Centre and Internews for their support throughout the duration of the project. Additionally, appreciation is extended to MISA Lesotho for their contribution towards the launch of this report. Special recognition is extended to the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information in Africa, Honourable Commissioner Ourveena Geereesha Topsy-Sonoo, for supporting the research initiative and her generous contribution to the report by providing its preface. This work was carried out with funding support from USAID under the ARISA programme, administered by Freedom House.

Photo acknowledgments:

Shutterstock
Adobe Stock

Design and layout:

Busisiwe I. Crafford, Centre for Human Rights

The Centre for Human Rights

The Centre for Human Rights is an internationally recognised institution based at the Faculty of Law at the University of Pretoria. It is both an academic and human rights organisation that aims to contribute to advancing human rights through education, research, and advocacy.

The Transformation Resource Centre

The Transformation Resource Centre (TRC) is a membership based civil society organisation mandated to oversee issues of governance and promotion and respect for human rights through advocacy, campaigns, research and strategic litigation. TRC also promotes Human Rights, Access to Justice, and Social Accountability by ensuring that information is digitally available to communities and authorities through TRC media outlets.

ARISA Programme

This work was conducted with the support of Freedom House under the Advancing Rights in Southern Africa (ARISA) programme. The goal of the ARISA programme is to improve the recognition, awareness, and enforcement of human rights in the region and a cross-cutting emphasis on protecting the region's most vulnerable and marginalised groups, including indigenous peoples, women, and youth.

INSPIRES Project

Internews, with funding from USAID, was leading a consortium of seven members to implement the INSPIRES project, Enabling and Protecting Civic Space. The project aimed to increase knowledge and capacity to respond to growing restrictions on democratic freedoms of association, assembly, and expression. As civic space shifts rapidly around the globe, Internews believes that faster and more potent interventions are critical for strengthening local civil societies.

Preface

I welcome this important assessment of the state of digital rights in Lesotho. Through comprehensive examination, the study provides an in-depth analysis of the recognition of digital rights and spotlights various digital human rights violations and infringements experienced by the people in Lesotho. Through rigorous analysis and thoughtful exploration, it highlights the complexities and challenges inherent in safeguarding digital rights on the continent, thereby informing policy-making, shaping legal frameworks, and fostering greater awareness and advocacy on digital rights issues in Lesotho and beyond. The study is an extension of the Digital Rights in Southern Africa project that was undertaken by the Centre for Human Rights in 2022 and 2023. By building upon the foundational work of this comprehensive initiative, the current study seeks to deepen understanding of digital rights issues in the African context, particularly through the lens of the Lesotho experience.

Despite notable advancements in efforts to narrow the digital divide in Lesotho, the emergence of the COVID-19 pandemic exposed the persistent challenges, both online and offline. While many societies worldwide have embraced the opportunities presented by the digital age, regions of the global south continue to grapple with a plethora of digital threats and negative effects, which disproportionately impact vulnerable and marginalised segments of the population. Regrettably, Lesotho is not immune to these trends of exclusion and further marginalisation. The proliferation of digital technologies has precipitated a corresponding increase in the incidence of human rights violations.

This report undertakes a comprehensive examination of the strategies and initiatives implemented in Lesotho, by the government and relevant stakeholders to safeguard human rights in the digital age. Focusing on various aspects of human rights in the digital sphere, including but not limited to access to the internet, freedom of expression, cybersecurity, cybercrimes, data protection, and surveillance, this study provides a thorough assessment of the current landscape of digital rights in Lesotho. By scrutinising these critical dimensions, the report analyses the prevailing state of affairs and the level of accessibility to digital technologies within the country. It also seeks to contribute substantially to the ongoing global discourse surrounding digital rights by shedding light on the specific challenges and opportunities encountered in the global south. As developing nations navigate the complexities of the digital age, it is essential to identify gaps and explore potential mechanisms for safeguarding and promoting digital rights in these contexts. This report seeks to contribute meaningfully to this dialogue and advocate for the protection and enhancement of digital rights for all individuals, regardless of geographical location or socio-economic status.

The effective implementation of the recommendations proposed in this report holds the promise of yielding substantial improvements to the digital rights landscape in Lesotho. It is important that government agencies, civil society organisations, the private sector, academia, and the broader community unite in a concerted effort to address the identified challenges and implement the proposed solutions. I therefore urge all key stakeholders in Lesotho to carefully consider these insights and recommendations and engage in collaborative efforts within the respective spheres of influence to enhance the digital rights in the country. Initiatives conducted synergistically can affect meaningful change and ensure that digital rights are upheld and protected for all citizens, particularly those who are marginalised or vulnerable. By heeding the proposed actions, policymakers and stakeholders can proactively address existing gaps and challenges, thereby promoting an environment that is more conducive to the realisation of digital rights promotion and protection of digital rights will not only empower

marginalised groups but also enhance inclusivity, equity, and social justice within the digital sphere. Ultimately, the successful implementation of these measures stands to catalyse positive societal transformation and pave the way for a more rights-respecting and digitally inclusive future for the people of Lesotho.

Finally, I wish to extend my sincere appreciation to the Centre for Human Rights, University of Pretoria and the Transformation Resource Centre for their admirable efforts in conducting this comprehensive analysis of the state of digital rights in Lesotho. Their dedication to advancing human rights and promoting digital inclusion is commendable, and their contributions to this field are invaluable. I applaud their commitment to conducting rigorous research and providing targeted and evidence-based recommendations that will undoubtedly serve as a catalyst for positive change.

Honourable Commissioner Ourveena Geereesha Topsy-Sonoo

Special Rapporteur on Freedom of Expression and Access to Information in Africa, African Commission on Human and Peoples' Rights

Glossary of Abbreviations

African Charter	African Charter on Human and Peoples Rights
AI	Artificial Intelligence
ACHPR	African Commission on Human and Peoples' Rights
ACRWC	African Charter on the Rights and Welfare of the Child
ACERWC	African Committee of Experts in the Rights and Welfare of the Child
AU	African Union
CEDAW	Convention on the Elimination of All Forms of Discrimination against Women
ChatGPT	Chat Generative Pretrained Transformer
CRC	Convention on the Rights of the Child
CRPD	Convention on the Rights of Persons with Disabilities
CSAM	Child Sexual Abuse Material
DPA	Data Protection Act
ETL	Econet Telecom Lesotho
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICT	Information and Communications Technology
ISP	Internet Service Providers
IT	Information Technology
IoT	Internet of Things
LCA	Lesotho Communications Authority
LGBTQIA	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, and Asexual
NSDP II	National Strategic Development Plan
NCSAC	National Cyber Security Advisory Council
SMMEs	Small, Medium and Micro Enterprises
OAU	Organisation of African Unity
PWD	Persons with Disabilities
SDGs	Sustainable Development Goals
SADC	Southern African Development Community
SMS	Short Message Services
STEM	Science, Technology, Engineering, and Mathematics
UDHR	Universal Declaration of Human Rights
UN	United Nations
VCL	Vodacom Lesotho
NSDP	National Strategic Development Plan

CHAPTER 1
INTRODUCTION

1. INTRODUCTION

In this era of the Internet of Things (IoT), emerging technologies, artificial intelligence tools, decentralised databases, data management technologies and the 4th Industrial Revolution, computers are central to all essential activities either in personal spaces or workspaces. These developments have shifted individual lives from traditional locales onto digital and virtual platforms. General communication, financial transactions, payment systems, data storage, accounting, taxation, political organisation, civic activism, legal proceedings, education, science and business now take place online. This switch has been followed by complexities to the protection and promotion of fundamental freedoms and rights as well as safeguarding state security interests in cyberspace.For a more elaborate background, one need not look further than the 2015-2017 period. During this time, Lesotho witnessed the might of social media as a force for democratisation and government accountability. Digital platforms actualised freedom of expression, access to information, freedom to communicate ideas, freedom to protest and the right to associate online. Political campaigning, citizen 'journalism' and civic activism were revolutionised as digital platforms enabled and expanded political, media, and civic spaces.

In the ensuing climate, the then Deputy Prime Minister, Mothejoa Metsing, threatened to close Facebook because it was peddling misinformation that threatened government stability.[1] On Facebook, there was a page called Countdown to Elections 2015, 16 or 17 which amassed over 50 000 followers. The group was dominated by three pseudonyms, Makhaola Qalo, Lira Litjame, and Paul Sithole. These pseudonyms were notorious for leaking government data and exposing government plans as well as expressing critical views against the seven-party coalition government at the time. The government viewed social media as a security threat which had to be strictly regulated. With these developments, the efficacy of the internet was fairly witnessed. This was seen in its ability to facilitate communication between persons due to its speed, accessibility and non-recognition of geographical borders. It enabled individuals to express their opinions freely and to easily access information. The media and civic and political players contributed and benefited significantly. While societies benefit from internet use, some sections of the community, especially vulnerable and marginalised groups have limited access to the internet thus bordering on discrimination. These groups include Persons With Disabilities (PWDs), women and rural communities. It is therefore crucial for states to narrow the digital divide and ensure equal access to the internet for overall public benefit.

This report is aimed at providing an account of the recognition of digital rights in Lesotho as mandated by the Constitution and international human rights laws and standards. It sets out the human rights framework that informs the protection of human rights. It examines human rights violations that occur through the use of the internet together with human rights infringements by measures that are meant to regulate the internet. It explores cybersecurity and its challenges in Lesotho, freedom of expression online and the effect of surveillance on digital rights. The report further provides statistical summaries on internet access and the digital divide that affects vulnerable groups in society. In conclusion, the report acknowledges Lesotho's achievements in the promotion and protection of human rights in the digital age and proposes recommendations to facilitate improvement. The report builds on the Centre for Human Rights, University of Pretoria's report on the status of digital rights in Southern Africa.[2]

1 'Minister wants Facebook Shut Down' *The Post* https://www.thepost.co.ls/local-news/minister-wants-facebook-shut-down/ (Accessed 30 August 2023).

2 Centre for Human Rights 'The digital rights landscape in Southern Africa' (2022) https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Digital_Rights_Landscape_in_SADC_Report.pdf (accessed 31 August 2023).

1.1 Objectives of the report

The central focus of this report is to undertake a comprehensive analysis of the digital rights landscape in Lesotho, anchored by four specific objectives. Firstly, it seeks to establish a fundamental understanding of human rights and the responsibilities of states concerning rights both offline and online. Secondly, it aims to evaluate the current state of digital rights in Lesotho across six key thematic areas: internet accessibility, cybersecurity, freedom of expression online, access to information, online communication surveillance, and the digital inclusion of vulnerable and marginalised groups. Additionally, the report scrutinises the existing regulatory framework pertinent to these thematic areas. Finally, it proposes actionable recommendations aimed at enhancing the promotion and protection of digital rights in Lesotho.

1.2 Methodology

The report employs a comprehensive desktop research approach, relying on textual analysis of human rights instruments adopted at the international, continental and subregional levels. Key instruments scrutinised include the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the African Charter on Human and Peoples' Rights (African Charter) and other relevant hard and soft laws. It also analyses the domestic framework which consists of statutes, regulations and rules on the recognition of human rights and regulation of the digital economy, and their compliance with the international instruments. These include the Constitution of Lesotho Order 5 of 1993 (Constitution),[3] the Data Protection Act Act 5 of 2011(DPA),[4] the Communications (Subscriber Identity Module Registration) Regulation 141 of 2021 (Communication Regulations) [5] and the Computer Crime and Cybersecurity Bill.[6] To enrich the analysis, the study also draws from a spectrum of scholarly literature, reports, newspaper articles and proceedings, offering a nuanced evaluation of Lesotho's adherence to human rights principles within the digital realm. By reflecting on the Lesotho legal system, the study derives valuable lessons on the best human rights-based approaches for the protection and promotion of human rights in the digital age, including the regulation of cyberspace.

1.3 Key findings: framing digital rights in Lesotho

Access to the internet in Lesotho is on the rise, yet it faces significant hurdles stemming from its Information and Communication Technology (ICT) infrastructure, the affordability of internet services and devices, and a lack of widespread ICT proficiency. Despite the manifold advantages the internet offers, its usage can encroach on fundamental human rights. These violations often arise from cybersecurity threats compromising users' privacy rights, surveillance via data collection, among other factors. Safeguarding human rights online, or digital rights, is important for leveraging the internet's full potential. Consequently, regulations governing internet and digital technologies should be implemented, ensuring compliance with established international human rights standards.

---

3 Constitution of Lesotho Order 5 of 1993 with Amendments through 2011 https://www.gov.ls/download/lesotho-constitution/ (accessed 01 September 2023).

4 Data Protection Act 5 of 2011 https://www.centralbank.org.ls/images/Legislation/Principal/Data_Protection_Act_2011.pdf (accessed 01 May 2023).

5 Communications (Subscriber Identity Module Registration) Regulation 141 of 2021 https://lca.org.ls/wp-content/uploads/filr/3229/SIM%20CARD%20REGISTRATION%20REGULATIONS%202021%20(2).pdf (accessed 01 May 2023).

6 Computer Crime and Cybersecurity Bill of 2023.

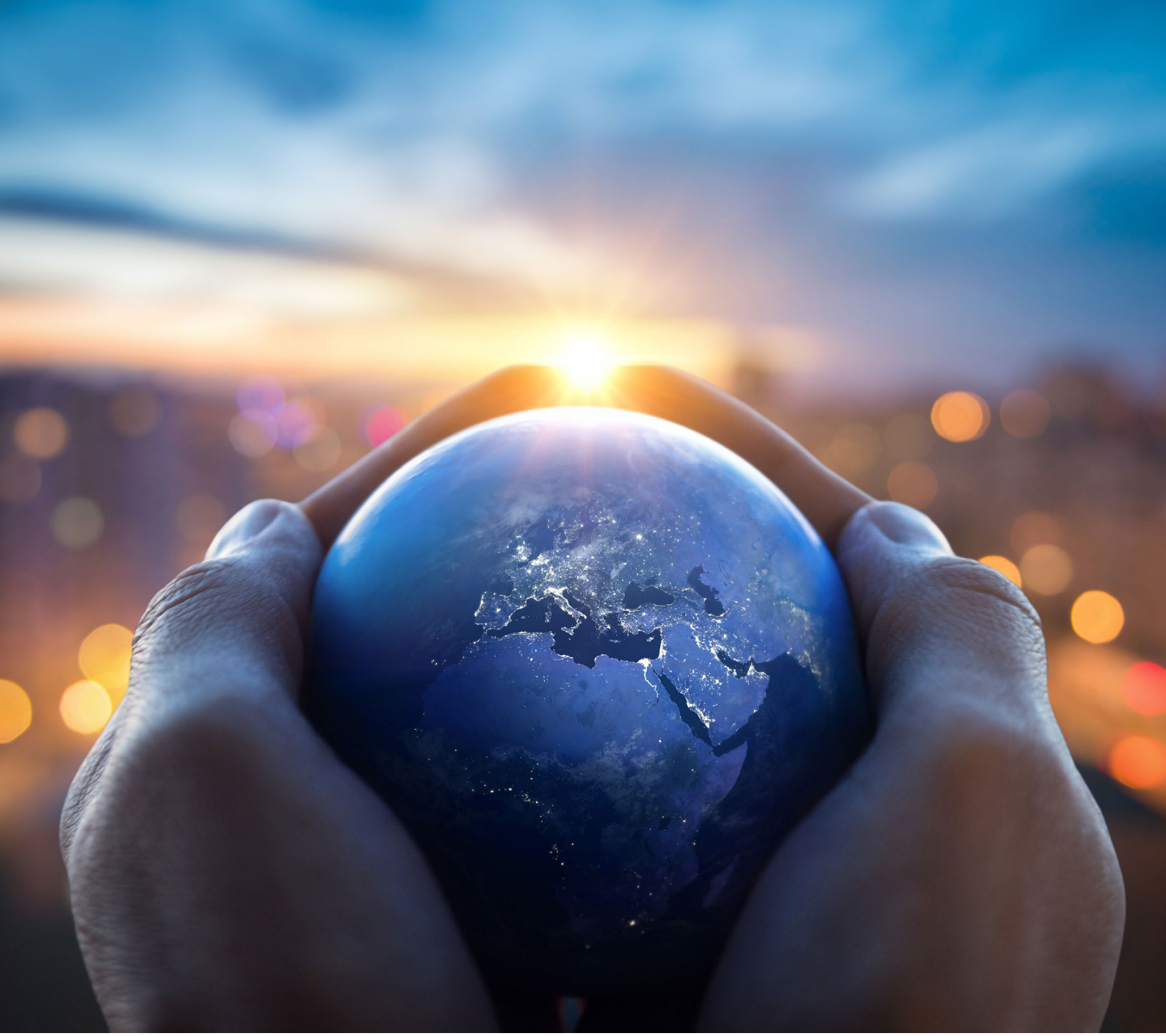
The Constitution guarantees human rights and freedoms offline as set out by international human rights standards. Yet, while strides have been made to extend these protections to the digital sphere, the legislative landscape still falls short in fully safeguarding human rights online. For instance, while the Data Protection Act ostensibly ensures data protection in accordance with global human rights norms, the absence of a robust regulatory body, such as a Data Protection Authority (DPA), hampers effective oversight and enforcement, leaving a gap in ensuring compliance with these crucial protections.

While the Computer Crime and Cyber Security Bill is aimed at safeguarding internet users, it has faced criticism for its inclusion of provisions that potentially infringe upon human rights. Specifically, the Bill has been faulted for reintroducing criminal defamation through the criminalisation of false dissemination of information. Furthermore, its vague definition of "illegal access" also raises concerns about its potential to unreasonably curtail freedom of expression. The Bill aims to empower authorities to investigate computer crimes using forensic tools, subject to judicial oversight. Its passage would achieve a critical equilibrium between combating cyber offences and upholding digital rights. This balance has remained elusive in existing legislation like the Penal Code, the Communications Act, and the National Security Services Act.[7]

In addition, the report shows the indispensable role of the media in a democratic society. In Lesotho there is a visible presence of a vibrant and varied media landscape across both offline and online platforms. However, while regulations such as the Broadcasting Code[8] and the Public Health (COVID-19) (Risk Determination and Mitigation Measures) Regulations[9] prohibit publication of misinformation, disinformation and hate speech,[10] they may compromise the rights and independence of the media.

While Lesotho boasts relatively high internet accessibility, particularly in urban centres, achieving universal access faces hurdles such as prohibitive device costs, limited electricity access, and exorbitant data expenses. These challenges disproportionately hinder internet connectivity in rural locales. Vulnerable demographics, notably women and persons with disabilities (PWDs), bear the brunt of these disparities. Despite the government's 2016 attempt to enforce internet disruptions, there have been no documented instances of successful implementation. While emerging technologies have promoted economic growth, there are concerns surrounding their potential adverse effects on certain human rights. A discussion of the foundation of human rights and states' obligations follows as a basis for the assessment of digital rights in this report.

7 National Security Services Act 11 of 1988 http://www.vertic.org/media/National%20Legislation/Lesotho/LS_National_Security_Services_Act.pdf (accessed 02 May 2023).
8 Broadcasting Code 38 of 2022 https://lca.org.ls/wp-content/uploads/filr/3237/BROADCASTING%20CODE%202022%20final%20(2)%20(1).pdf (accessed 04 May 2023).
9 Public Health (COVID-19) (Risk Determination and Mitigation Measures) Regulation 2 of 2021 https://www.gov.ls/wp-content/uploads/2021/01/COVID-GAZETTE-140121.pdf (accessed 03 May 2023).
10 Rule 7 & 17 Broadcasting Code



CHAPTER 2
INTERNATIONAL HUMAN RIGHTS FRAMEWORK ON DIGITAL RIGHTS

2. INTERNATIONAL HUMAN RIGHTS FRAMEWORK ON DIGITAL RIGHTS

A human right is a moral claim that a person can raise by virtue of being a human being with inherent dignity.[11] The interrelations between humans require mutual respect for the other's human dignity and life.[12] Human dignity is therefore at the centre of the human rights regime.12 Human rights are implemented based on principles that they are 'universal, indivisible and interdependent and interrelated.'[13] Universality implies that all humans in the world are entitled to claim a dignified existence, without discrimination. Characteristics such as race, sex, or social position are irrelevant to their entitlement to human rights.[14] Further, human rights are indivisible in that one right may invoke/imply another right.[15] For instance, freedom of association implies freedom of assembly. Moreover, the effective implementation of one right may depend on the implementation of another right.[16] For example, freedom from arbitrary arrest invokes the right to equal protection of the law. It follows that each right relies on and complements the other. Thus, violation of one right might mean violation of another that is dependent on the first right. The international human rights framework comprises standards contained in agreements and principles set by states to promote and protect the rights and dignity of all individuals. It is inclusive of a wide range of rights inherent to all human beings regardless of their nationality, race, religion, gender or any other status. In the context of Lesotho, adherence to these standards occurs across multiple tiers, including the global level through the United Nations (UN), the regional level via the African Union (AU), and the subregional level through the Southern African Development Community (SADC). The standards in each of these levels are discussed below:

2.1 United Nations framework

The genesis of the UN human rights framework can be traced back to its inception in 1945, emerging in response to the grave atrocities against human dignity witnessed during World War II. In the aftermath of the conflict, states united in their determination to establish a robust moral edifice aimed at safeguarding the inherent dignity of all individuals.[17] This collective resolve materialised in the form of a comprehensive human rights framework, marking the commencement of a global endeavour to enshrine fundamental rights and freedoms. The process of international recognition of human rights began with the adoption of the UN Charter in 1945 where the UN agreed that 'all people matter.'[18] Subsequently, the UN undertook the momentous task of codifying these principles, culminating in the adoption of three pivotal instruments: the Universal Declaration of Human Rights (UDHR) in 1948, followed by the

11 F Viljoen *International Human Rights Law in Africa* (2012) 3. Nowak defines human rights as "[t]hose fundamental rights, which empower human beings to shape their lives in accordance with liberty, equality and respect for human dignity." M Nowak *Introduction to the International Human Rights Regime* (2003) 1.

12 Viljoen (n 11) 4.

13 United Nations 'Note/by the Secretariat A/CONF.157/23: Vienna Declaration and Programme of Action Note/by the Secretariat' (1993) para 5 https://digitallibrary.un.org/record/183139?ln=en&v=pdf (accessed 01 July 2023).

14 JW Nickel *Making Sense of Human Rights* (1987) 3 & 28.

15 Viljoen (n 11) 327.

16 Nickel (n 14) 133.

17 CJ Hamelink 'Human rights in cyberspace' in D Haenens (eds) *Cyberidentities Canadian and European Presence In Cyberspace*. (1999) 31-46 https://books.openedition.org/uop/1372?lang=en (accessed 01 July 2023).

18 As above.

International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR) in 1966.

The three UN instruments, which are referred to as the International Bill of Rights, contain several human rights including the right to life,[19] freedom from torture,[20] right to liberty,[21] right to equality before the law and equal protection of the law without discrimination,[22] right to a fair trial,[23] right to privacy,[24] freedom of expression,[25] freedom of assembly and association,[26] right to political participation,[27] right to work,[28] right to education,[29] right to free and fair elections[30] and right to health.[31]

2.2 Regional and Subregional Human Rights Framework

At the regional level, African countries established the Organisation of African Unity (OAU), which adopted the African Charter on Human and Peoples' Rights (the African Charter) in 1981. The African Charter guarantees civil and political rights and socio-economic rights and expounds on the rights of peoples and duties of individuals.[32] It came into force in 1986. The OAU was replaced by the African Union (AU) in 2002. Other examples of regional instruments are the African Charter on the Rights and Welfare of a Child (ACRWC)[33] and the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (the Maputo Protocol). In addition, the AU has adopted numerous instruments and soft laws in the promotion of human rights, which are explored later. At a subregional level, the SADC also adopted legal instruments that guarantee and promote human rights. An example is the SADC Model Law on Data Protection 2013.[34]

2.3 Protection of human rights in the cyberspace

According to the principles of human rights solidarity, the relationship between cyber security and human rights can be complex and multifaceted as the internet and other digital technologies have become increasingly crucial for the exercise of many human rights. Recognizing the alarming instances of human rights violations in cyberspace perpetrated by both governments and non-state actors, the UN has acknowledged the significance of safeguarding human rights in the online realm.[35] Upholding human dignity is important both offline and online.

19 Article 3 UDHR; Article 6 ICCPR.
20 Article 5 UDHR; Article 7 ICCPR.
21 Article 9 UDHR; Article 9 ICCPR.
22 Article 7 UDHR; Article 25 ICCPR.
23 Article 10 UDHR; Article 14 ICCPR.
24 Article 12 UDHR; Article 17 ICCPR.
25 Article 19 UDHR; Article 19 ICCPR.
26 Article 20 UDHR; Article 21 & 22 ICCPR.
27 Article 21 UDHR; Article 25 ICCPR.
28 Article 23 UDHR; Article 6 ICESCR.
29 Article 26 UDHR; Article 13 ICESCR.
30 Article 25 ICCPR.
31 Article 12 ICESCR.
32 Viljoen (n 11) 12.
33 African Union 'African Charter on the Rights and Welfare of a Child' (1990) https://au.int/sites/default/files/treaties/36804-treaty-0014__african_charter_on_the_rights_and_welfare_of_the_child_e.pdf (accessed 11 August 2023).
34 HIPSSA *Data Protection: Southern African Development Community Model Law* (2013) https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf (accessed 12 March 2024).
35 MI Franklin 'Human Rights future for the Internet' in M Ketteman (eds) *Research Handbook on Human*

Consequently, the UN General Assembly therefore committed to creating an inclusive, people-centred information society that aligns with and respects the principles of the UDHR.[36] In 2016, the UN reiterated the principle that 'the same rights that people have offline should also be protected online.'[37] This paradigm of 'human rights in the internet era' is encapsulated by the concept of digital rights, which serve as an extension of traditional human rights tailored to the demands of the digital age.[38]

The UN Joint Declaration on Freedom of Expression and the Internet, for example, spotlights the significant role of the internet in empowering billions worldwide by amplifying their voices, facilitating access to information, and enhancing their capacity for reporting. Based on this, promoting and safeguarding freedom of expression and the right of access to information in the digital sphere is important.[39] While the ICCPR does not expressly address the realisation of freedom of expression in a digital space, Article 19 is expansively formulated to ensure the exercise of this fundamental right through any chosen medium. The Human Rights Committee, in its General Comment 34, further elaborated on Article 19, emphasising the indispensable nature of freedom of opinion and expression for promoting transparency and accountability within societies. Additionally, the scope of this right is wide and includes political discourse, canvassing, teaching, discussion of human rights, and journalism through various means including 'electronic and internet-based modes of expression.'[40]

Accordingly, the AU has proactively developed frameworks to safeguard human rights in the digital realm. Notable among these is the Convention on Cyber Security and Personal Data Protection (the Malabo Convention)[41]; the African Commission on Human and Peoples' Rights (ACHPR) Resolution on the Right to Freedom of Information and Expression on the Internet,[42] of 2016; and the ACHPR Declaration on Principles of Freedom of Expression and Access to Information in Africa of 2019 (2019 ACHPR Declaration).[43] The Declaration outlines 43 key principles aimed at ensuring freedom of expression and access to information across both online and offline platforms. Furthermore, the African Declaration on Internet Rights and Freedoms recognises and emphasises the role of the internet as an empowering space for human rights fulfilment. Central to this declaration are fundamental rights such as the right 'to hold opinions without interference, the right to freedom of expression and information, the right to freedom of assembly and association, the right to freedom of thought, conscience and religion, the right to be free from discrimination in all forms'.[44] The Model Law on Access to Information for

Rights and Digital Technology: Global Politics, Law and International Relations (2019) 7.

36 Franklin (n 35) 5.

37 United Nations Human Rights Council 'Resolution A/HRC/RES/32/13 2016: Resolution on the promotion, protection and enjoyment of human rights on the Internet' 18 July 2016 32nd Session Geneva, para 1.

38 R Hutt 'What are your digital rights' *World Economic Forum* 13 November 2015 https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/ (accessed 05 May 2023).

39 United Nations Human Rights Special Procedures *et al ' Joint Declaration on Freedom of Expression and Elections in the Digital Age*' https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclarationDigitalAge_30April2020_EN.pdf (accessed 06 May 2023).

40 United Nations 'General Comment 34 CCPR/C/GC/34: General Comment 34 of the International Covenant on Civil and Political Rightson Freedom of opinion and expression' (2011) para 12. https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (accessed 07 May 2023).

41 African Union 'Convention on Cyber Security and Personal Data Protection' (2014) https://au.int/sites/default/files/treaties/29560treaty0048__african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 08 May 2023). Lesotho has not yet ratified the Convention.

42 ACHPR 'Resolution ACHPR/Res 362 (LIX) 2016: Resolution on Right to Freedom of Information and Expression on the Internet.' It gives effect to article 9 of the African Charter on the digital era.

43 The ACHPR's Declaration on Principles of Freedom of Expression and Access to Information in Africa adopted in 2002 and revised in 2019.

44 African Internet Rights 'African declaration on internet rights and freedoms' https://africaninternetrights.

Africa[45] and the ACHPR Guidelines on Access to Information and Elections[46] have been instituted to reinforce the right of access to information as guaranteed under international human rights laws and standards. At the subregional level, SADC developed model laws that are crucial for navigating the complexities of the digital era: the SADC Model Law on Computer Crime and Cybercrime 2013, and SADC Model Law on Electronic Transactions and Electronic Commerce 2013 among others.[47] These efforts are indicative of the continent's commitment to upholding human rights in the digital age, ensuring that individuals across Africa can fully exercise their rights both online and offline.

2.4 States' obligations towards all human rights

Governments are obliged to respect, protect, fulfil, and promote human rights of all equally without distinction.[48] Similarly, they are tasked with honouring human rights by enabling individuals to freely exercise their entitlements without undue interference.[49] For example, the state should refrain from curtailing freedom of expression which includes the right of individuals to freely express their opinions. Any unwarranted encroachments on these rights is regarded as human rights violations.[50] To ensure the protection of human rights, governments are required to adopt measures including legislative frameworks, to prevent violations by both private entities and governmental bodies. Thus, not only governments but individuals as well have a duty to uphold these rights and refrain from infringing upon the rights of others.[51] Moreover, fulfilling these rights necessitates proactive steps from governments to ensure their citizens can fully enjoy them.[52] This might involve initiatives like constructing schools to facilitate access to education—a fundamental human right.

Additionally, governments have a crucial role in promoting awareness and understanding of human rights among the populace.[53] Through the ratification of international human rights instruments, governments commit to upholding and safeguarding the rights of all individuals within their jurisdiction, without distinction of any kind such as race, sex, birth or other status.[54] States should ensure that human rights are upheld on the internet just as they are in the physical world, including respect, fulfilment, protection, and promotion. This necessitates the implementation of legal frameworks and other measures to safeguard internet users from digital rights infringements, including cybercrimes. However, some regulations run the risk of encroaching upon the very rights they aim to safeguard. Therefore, it is crucial for states to find a delicate balance between combating digital offences and guaranteeing the protection and promotion of digital rights.

org/sites/default/files/African-Declaration-English-FINAL.pdf (accessed: 03 August 2023) See also APAI 'African platform on access to information' (2011) http://www.oas.org/es/sla/ddi/docs/acceso_informacion_desarrollos_UA_platform.pdf (accessed: 02 August 2023).

45 ACHPR 'Model law on access to information for Africa'(2013) https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/model_law_on_ati_in_africa/model_law_on_access_to_infomation_en.pdf (accessed 01 August 2023).

46 ACHPR 'Guidelines On Access to Information And Elections in Africa'(2013) https://achpr.au.int/en/node/894 (accessed 12 March 2024).

47 SADC 'Model law on computer crime and cybercrime' (2013). https://www.veritaszim.net/sites/veritas_d/files/SADC%20Model%20Law%20on%20Computer%20Crime%20and%20Cybercrime.pdf (accessed 30 July 2023).

48 Nowak (n 11) 27; Viljoen (n 11) 6.

49 Article 2 ICCPR, member states of the ICCPR undertake to respect and ensure rights in the convention.

50 Nowak (n 11) 49.

51 Nickel (n 14) 3.

52 Nowak (n 52).

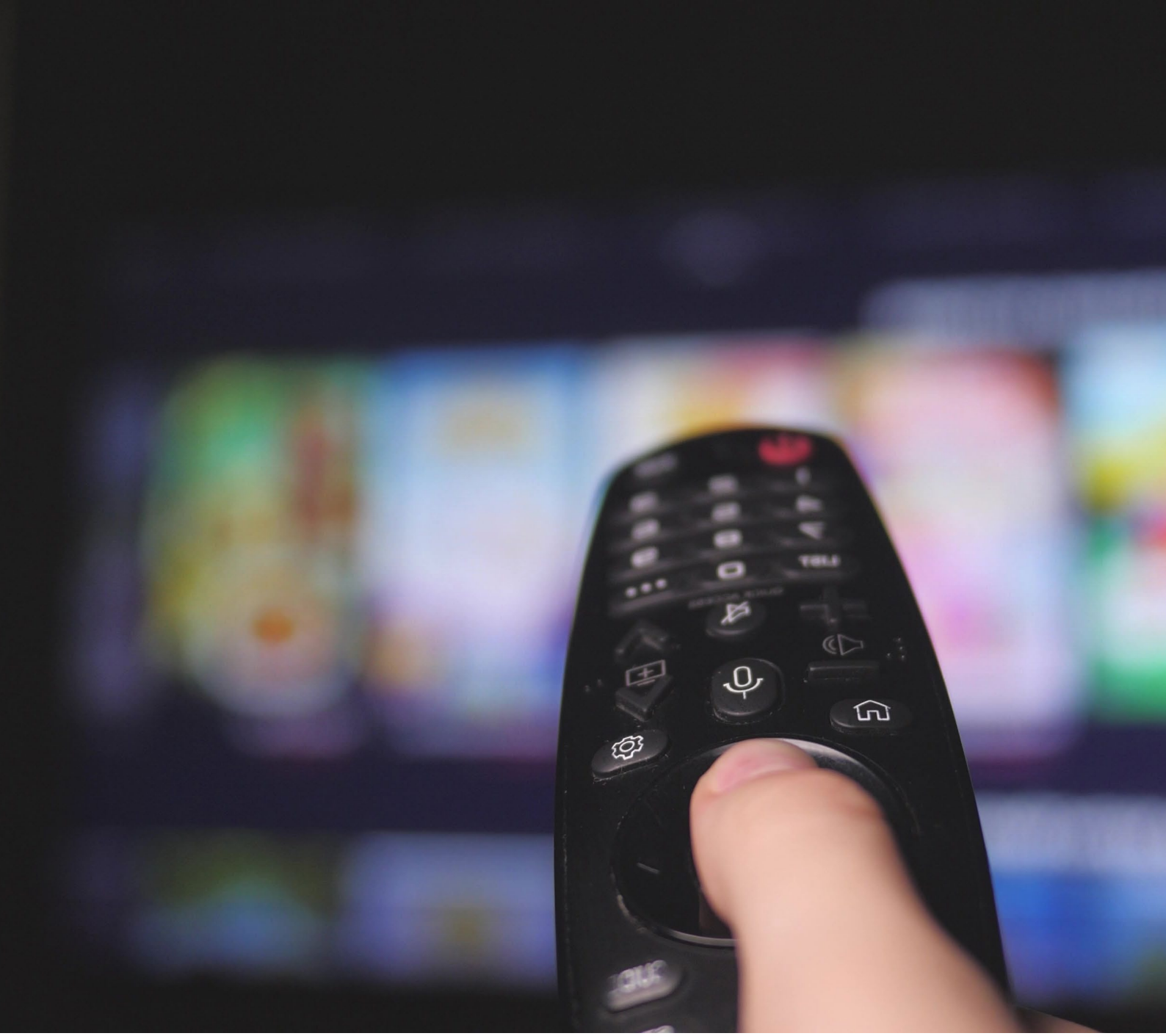
53 Viljoen (n 50).

54 Article 2 ICCPR.

2.5 Limitations of human rights

Though human rights are legally protected, most rights are not absolute and can be subject to justifiable limitations. A limitation should be lawful; serve a particular objective such as balancing human rights with state security or public order; preserve the rights of another; or any legitimate purpose.[55] To justify the limitation, the impact it has on human rights should be carefully weighed against the legitimate state interest being pursued. The negative impact of the limitation should be outweighed by the importance of the state interest. Additionally, the limitation should be deemed necessary and proportionate in relation to achieving its intended goal. Before analysing Lesotho's protection of digital rights, it is prudent to provide a national context of the state of internet access.

55 General Comment 34 (n 40) para 21-36; Viljoen (n 11) 330; Article 27 (2) of the African Charter.



CHAPTER 3
UNIVERSAL ACCESS TO THE INTERNET

3. UNIVERSAL ACCESS TO THE INTERNET

The African Union Declaration on Internet Access,[56] calls on states to develop an 'accessible and affordable internet' to enable people to fully benefit from its potential and transformative capabilities. States should therefore formulate comprehensive policies and strategies aimed at bridging the digital divide, which refers to the gap between those who enjoy unrestricted internet access and those who are marginalised by its absence. Digital inclusion encompasses activities that secure equal internet access for all individuals, particularly those from disadvantaged backgrounds.[57] Several factors contribute to the digital divide. Firstly, the availability of internet infrastructure in a given area plays a crucial role. Secondly, affordability is a significant determinant; if the cost of data outweighs the affordability threshold, internet access becomes elusive. If the cost of data is high compared to essential goods, the internet becomes less accessible. Thirdly, the quality of internet service is important, determined by factors such as upload and download speeds; and sluggish connectivity which inhibits effective usage. Additionally, the relevance of internet content to a community impacts accessibility; content not aligned with community needs or in an unfamiliar language poses barriers. Lastly, individual digital literacy and proficiency in using technology are essential.[58] Lacking these skills can hinder internet access, highlighting the importance of e-skills development initiatives.

3.1 Access to the internet in Lesotho

In 2017, out of fourteen SADC countries, Lesotho was ranked the fifth country with a high mobile penetration rate.[59] It was ranked fourteen in Africa by 2022.[60] Datareportal findings as of February 2023, reveal that there were 1.11 million internet users in Lesotho out of a population of 2.32 million, marking a 48% internet penetration rate[61] while leaving 52% unconnected. Over time, there has been a steady rise in internet usage in Lesotho. From 2005 to 2010, there was a 1% increase, followed by a notable 21% surge from 2010 to 2015, and an additional 18% growth from 2015 to 2020.[62] Among internet users, a significant 86% access the internet via smartphones, reflecting the widespread adoption of mobile technology.[63] Impressively, active mobile connections stand at 104.8% of the population, totaling 2.43 million connections, attributed to multiple gadget ownership.[64] Notably, 90% of internet users in Lesotho rely on 3G connections.[65] Currently, there are at least 489.5 thousand social media users in Lesotho,

56 African Union 'Declaration on Internet Access' https://au.int/sites/default/files/newsevents/workingdocuments/33025-wd-african_declaration_on_internet_governance_en_0.pdf (accessed 30 July 2023).

57 The Centre for Digital Equity 'What is digital inclusion?' https://thecenterfordigitalequity.org/what-is-digital-inclusion/ (accessed 30 May 2023).

58 C Muller & J Aguiar 'What Is the Digital Divide?' *Internet Society* 3 March 2022. https://www.internetsociety.org/blog/2022/03/what-is-the-digital-divide/#:~:text=At%20a%20high%20level%2C%20the,affordability%2C%20quality%2C%20and%20relevance (accessed 30 May 2023).

59 Lesotho Communications Authority 'The state of ICT in Lesotho' (2017) https://researchictafrica.net/wp/wp-content/uploads/2018/01/2017_The-State-of-ICT-in-Lesotho_RIA_LCA.pdf (accessed 07 May 2023).

60 Statista 'Share of internet users in Africa as of January 2024, by country' https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/ (accessed 25 May 2023).

61 S Kemp 'Digital 2023: Lesotho' *Datareportal* 14 February 2023 https://datareportal.com/reports/digital-2023-lesotho (accessed 07 May 2023).

62 The World Bank 'Individuals using the Internet (% of population)–Lesotho'. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=LS&most_recent_value_desc=false (accessed 07 May 2023).

63 A Gillwald & O Mothobi 'Low internet penetration despite 90% 3G Coverage in Lesotho *'Research ICT Africa* August 2017 https://researchictafrica.net/publication/low-internet-penetration-despite-90-3g-coverage-in-lesotho/ (accessed 07 May 2023).

64 Kemp (n 61).

65 MISA 'The state of press freedom in Southern Africa 2022' (2022) 44 https://data.misa.org/api/

constituting 21.2% of the population,[66] indicating an upsurge in internet penetration in the country. Also, the average speed of fixed internet connections stands at 17.33Mbps, marking a significant 26.9% increase from the beginning of 2022 to 2023, indicative of improving connectivity infrastructure and services.[67] Access to the internet in Lesotho is directly affected by the ICT infrastructure in the country as explored below.

3.2 ICT Infrastructure in Lesotho

Effective ICT infrastructure comprises multiple essential components, including a significant inventory of computers and mobile phones, robust connectivity infrastructure with global access, and widespread availability of electricity to support a broader population.[68] Additionally, proficient monitoring skills are required to ensure the smooth operation and maintenance of this infrastructure. Lesotho predominantly had fixed network infrastructure. However, the fixed network inhibited the promotion of ICT access as network connections to homes were costly. There was a shift to a combination of fixed and wireless infrastructure. As of 2023, the wireless infrastructure is the dominant one. This strategic shift has catalysed the expansion of high-speed internet access,[69] with broadband now reaching an impressive 96% coverage in inhabited areas across Lesotho.[70]

Despite the strides made in expanding wireless infrastructure, challenges persist for internet users residing in underserved communities, particularly rural areas lacking reliable access to electricity. This absence of power sources poses a significant challenge for users seeking to charge their gadgets, including the internet-enabled ones. Econet Telecom Lesotho (ETL), a key network operator in the country, sought to address this issue by offering solar panel chargers for sale. However, despite these efforts, sales were insufficient to sustain the business model effectively.[71] As of the beginning of 2023, a notable demographic divide was evident, with 30.2% of the population residing in urban areas, while the majority, comprising 69.8%, inhabited rural areas.[72] This demographic distribution reaffirms the reality that a significant portion of the population in rural areas remains underserved by internet access, highlighting the persistent digital divide within the country.

The accessibility of ICT infrastructure in Lesotho is further hindered by the steep prices of smartphones. In response to this challenge, Vodacom Lesotho (VCL), a prominent network operator, introduced an initiative offering budget-friendly Smart Kicker phones priced at M400 (approximately US$22). This initiative has facilitated increased smartphone ownership among the population. Despite these efforts, however, the overall affordability of smartphones remains a significant barrier for many individuals in Lesotho due to the prohibitively high cost.[73]

Insufficient digital literacy exacerbates challenges within Lesotho's ICT infrastructure. A study conducted by the Lesotho Communications Authority (LCA) in 2016 utilised questionnaires to dissect the local ICT landscape. The study involved a survey of internet usage patterns of

files/1683794544953dragdlzlsfg.pdf (accessed 25 May 2023).

66 Kemp (n 61).
67 As above.
68 LCA (n 61)23.
69 LCA (n 61)25.
70 As above.
71 As above.
72 Kemp (n 69).
73 LCA (n 72).

households and individuals.[74] Alarmingly, 60% of non-internet users cited their lack of familiarity with digital tools as the primary reason for abstaining.[75] This dearth in e-skills correlates with a stagnant mobile broadband adoption rate.[76] Despite strides in internet connectivity, Lesotho's ICT backbone remains constricted due to prohibitive device costs, limited electricity accessibility, and a deficiency in digital competencies. Moreover, the affordability factor stands out as a significant determinant in shaping internet accessibility within Lesotho.

3.3 Affordability of internet

The accessibility of the internet hinges on the affordability of both devices and usage costs.[77] In Lesotho, this affordability is particularly strained, with the price of 1GB of data accounting for 3% of the average monthly salary.[78] Moreover, this burden is exacerbated across different sectors: while it represents 10% of a manufacturing worker's income, it still accounts for a significant portion (3%) of a technician's or a professional's earnings. A survey conducted by the LCA in 2016 revealed that a substantial 40% of individuals in Lesotho feel constrained by the high cost of data, undermining their internet usage. Despite these challenges, there is a notable upward trend in internet access across the country, albeit with greater penetration in urban areas compared to rural areas.

3.4 Internet disruptions and shutdowns in Lesotho

People have the ability to access information and share their viewpoints across various internet forums. However, during periods of heightened political tension, governments may resort to shutting down or interfering with internet access, effectively preventing the public from utilising these platforms. Internet Freedom Africa defined internet disruption which is often referred to as an internet shutdown as:

> the intentional blockage of access to the internet or sections of the internet such as social media platforms. Internet disruptions are mostly ordered by governments eager to disrupt communications and curtail citizens' access to information in order to limit what the citizens can see, do, or communicate.[79]

The social media platforms include blogs or social networking sites such as Facebook, X (formerly Twitter) and YouTube.

Internet-enabled communication empowers individuals to exercise their fundamental human right of freedom of expression. Due to the indivisible and interdependent nature of human rights, freedom of expression involves the freedom to hold opinions, communicate ideas, and also the essential right to seek, receive, and impart information without hindrance as enshrined in various international instruments and protected by the domestic framework.[80] In terms of the ICCPR, one may exercise the rights, 'regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.'[81] As indicated

74 LCA (n 61)43.
75 LCA (n 61)68.
76 LCA (n 61)27.
77 LCA (n 61)31.
78 LCA (n 61)34.
79 CIPESA 'Despots and Disruptions: Five Dimensions of Internet Shutdowns in Africa' (2019) https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/ (accessed 12 May 2023).
80 Section 14 (1) & 18 Constitution; Article 9 (1) African Charter; Article 19 UDHR.
81 Article 19 (2) ICCPR.

earlier, the UN has, through the Joint Declaration on Freedom of Expression and the Internet,[82] extended freedom of expression and the right to access information on the internet. However, when internet disruptions occur, they undermine these rights by stifling public discourse, frustrating participation in decision-making processes, and curtailing the dissemination of new information. In essence, such shutdowns constitute a violation of digital rights, including the freedom of expression and access to information.[83]

The Constitution guarantees freedom of expression.[84] The right may be subject to reasonable limitations in specific circumstances such as in the interests of national defence, public order, public safety, public health or morals, or for the protection of another's rights or reputation.[85] The ACHPR 2019 Declaration sets out justifiable limitations to freedom of expression and access to information. It states that a limitation is justifiable if it is prescribed by law; serves a legitimate aim; and is a necessary means to achieve the stated aim in a democratic society.[86] The Declaration further stipulates that states shall not interfere with the right to seek, receive and impart information through digital technologies by blocking or filtering content unless it is justiciable under international laws and standards.[87]

The Communications Act[88] which regulates telecommunications services and broadcasting services in Lesotho provides for internet disruptions. Section 20 asserts that licensees cannot be obstructed from delivering services unless their licence is revoked by the LCA or an emergency suspension order is issued by a Minister. Such an order should be founded on a credible belief that the licensee's ongoing operations jeopardise national security or public order, with no alternative recourse to mitigate the perceived threat other than shutting down operations. Consequently, the Act's regulation of freedom of expression falls within acceptable constitutional boundaries.

Although Lesotho has not experienced any documented internet disruptions, there have been two notable instances where such actions were attempted. In July 2016, ahead of the 2017 government elections, reports emerged indicating that the Lesotho government took a hostile stance towards social media platforms like Facebook and Twitter (now X), citing concerns that these platforms were divulging state secrets. The government suggested to the Lesotho Communications Authority (LCA) the shutdown of these social media networks. However, the LCA refused to endorse the proposal and insisted that the government provide a written order for such shutdowns. Without the assistance of LCA and Internet Service Providers (ISP), the government's attempts to enact the shutdowns were unsuccessful.[89] In November 2016, the

82 UN (n 39) para 1 (a).
83 N Pule 'Digital Rights in Lesotho: An analysis of the practices in the financial and ICT sectors' (2022) 32. https://rankingdigitalrights.org/wp-content/uploads/2022/07/Digital-Rights-in-Lesotho.pdf (accessed 09 May 2022).
84 Section 14 Constitution.
85 Section 14 (2) Constitution; Article 19 (3) ICCPR.
86 Principle 9 of ACHPR's 2019 Declaration.
87 Principle 38 of ACHPR's 2019 Declaration .
88 Communications Act 4 of 2012 https://media.lesotholii.org/files/legislation/akn-ls-act-2012-4-eng-2012-02-17.pdf (accessed 21 May 2023).
89 D McDevitt 'New report analyses internet censorship during Lesotho's 2017 general elections' *Open Technology Fund* 10 August 2017 https://www.opentech.fund/news/new-report-analyzes-internet-censorship-during-lesothos-2017-general-elections/ ; See also See also A Gwagwa 'When governments defriend social media: A study of Internet-based information controls in the Kingdom of Lesotho with a particular focus on the period around the 3 June 2017 General Elections'(2017) 5 https://www.opentech.fund/news/new-report-analyzes-internet-censorship-during-lesothos-2017-general-elections/. (accessed 10 May 2023)

government initiated a second attempt at shutting down social media platforms. It dispatched letters to Facebook and Twitter, demanding justification for why they should not face closure. However, the contents of the letters were leaked to the public, and the shutdown attempt failed.[90] Thus, the government's efforts to disrupt social media networks were futile on both occasions and the government did not succeed in disrupting digital rights through internet shutdowns. The subsequent section of the report analyses the cybersecurity regulation and the implications of digital rights in Lesotho.

90 McDevitt (n 89), See also MISA. 'Southern African Litigation Center: Navigating litigation during internet shutdowns in Southern Africa' (2019) 9-10. https://www.southernafricalitigationcentre.org/wp-content/uploads/2019/08/SALC-Internet-Shutdown-Guide-FINAL.pdf (accessed 10 May 2023).

CHAPTER 4
CYBERSECURITY, CYBERCRIME AND DATA PROTECTION

4. CYBERSECURITY, CYBERCRIME AND DATA PROTECTION

The section discusses the protection of digital rights in the context of cybersecurity, cybercrime and data protection.

4.1 Cybersecurity

Cybersecurity is 'the practice of protecting computers, electronic systems, networks and data from malicious attacks.'[91] It relates to the processes of protecting the confidentiality, integrity and availability of information in the cyber environment and the protection of internet users' assets.[92] Confidentiality of information relates to 'preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.'[93] Cybersecurity thus relates to the preservation of the right to privacy. Integrity of information relates to the assurance that information that is stored, in transit or being processed, is protected against improper alteration or destruction and the maintenance of its authenticity. This element relates to data protection. Availability denotes the swift and reliable access to information and its use.[94] Availability of information protects the right of access and free flow of information.

The protection of information and computer systems is achieved through a multifaceted approach, including encryption techniques, stringent user access controls, diligent hardware maintenance, and timely system upgrades to mitigate potential digital security threats.[95] The attacks on the data or internet users' assets often exploit vulnerabilities inherent in digital systems. Cybersecurity, therefore, offers one safeguard in cyberspace, ensuring, to a considerable degree, the preservation of privacy rights, access to information, and free flow of information can be guaranteed.[96]

The free flow of information in cyberspace, which is inextricably linked to freedom of opinion and expression, is important as it enables free interaction.[97] In the digital realm individuals with diverse perspectives convene to deliberate on matters of political and socioeconomic significance.[98] Therefore, safeguarding freedom of expression in cyberspace is crucial as it inherently safeguards the rights to assembly, association, and public participation.[99] The UN Special Rapporteur on the Freedom of Expression and Opinion emphasised the internet's pivotal role as a communication conduit facilitating the exercise of information rights enshrined in articles 19 of both the UDHR and ICCPR.[100] Reaffirming this stance, the UN upholds the principle

91 Kaspersky 'What is cyber security?' https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (accessed 02 June 2023).
92 MD Cavelty & C Kavanagh 'Cybersecurity and Human Rights' in B Wagner et al (eds.) Research Handbook on Human Rights and Digital Technology (2019) 75.
93 As above.
94 Cavelty & Kavanagh (n 92) 76.
95 As above; See also International Organisation for Standardisation 'ISO/IEC 27032:2012-Guidelines for cybersecurity' ISO/IEC 27032:2012 - Guidelines for cybersecurityiTeh Standards https://standards.iteh.ai › catalog › standards › iso-iec-2... (accessed 03 June 2023).
96 See Article 3 of the UDHR & Article 6 of the African Charter.
97 Article 9 African Charter.
98 Cavelty & Kavanagh (n 92) 86.
99 Article 10, 11 & 13 of the African Charter.
100 UN 'Report A/HRC/17/27: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue' (2011) https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/17/27 (accessed 04 June 2023).

that the rights enjoyed offline should be equally protected in the online sphere.[101]

In 2014, the AU adopted the Malabo Convention dedicated to addressing cybersecurity challenges on the continent. The Convention mandates member states to develop the requisite regulatory frameworks including the establishment of effective regulatory authorities. The regulatory bodies are envisaged to: recognise and identify threats to critical information infrastructure; develop national strategies to respond to cybersecurity attack incidents; conduct investigations and prosecutions where necessary; adopt cyber security monitoring structures; sensitise the public and build capacity on cybersecurity; and establish international co-operations on the matter.[102] Methods adopted by states in mitigating cybersecurity challenges should uphold basic human rights and freedoms.

Lesotho is grappling cybersecurity challenges, with phishing attacks,[103] hacking,[104] and social engineering tactics on the rise.[105] Additionally, the country faces heightened risks of cyber-attacks, including malware software attacks,[106] ransomware attacks,[107] Man in the Middle attacks,[108] denial of service attacks,[109] and data breaches which are the theft of data to commit crimes or espionage.[110] These cyber threats not only infringe upon established human rights and freedoms but also inflict significant financial losses upon businesses, individuals, and potentially governments.[111] In certain instances, cybersecurity breaches can escalate to pose threats to national security or public order, facilitating avenues for terrorist attacks and or cyber war.[112]

Research indicates that Lesotho is susceptible to cybersecurity attacks due to several key factors.[113] Firstly, the country faces challenges stemming from inadequate cybersecurity legislation, leaving gaps in regulatory frameworks necessary for robust protection. Secondly, there is limited awareness among the populace regarding cyber threats and the essential measures needed for protection against such risks. Thirdly, the existence of subpar infrastructure, exacerbating vulnerabilities and creating entry points for potential cyber breaches. Lastly, Lesotho contends with a shortage of skilled cybersecurity professionals equipped to effectively mitigate and respond to cyber attacks, further compounding its vulnerability in this rapidly evolving digital landscape.

101 UN 'Resolution A/HRC/RES/32/13: Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet' (2016) https://digitallibrary.un.org/record/845728?ln=en&v=pdf (accessed 04 June 2023).
102 Articles 24, 26-28 of UN Convention on Cyber Security and Personal Data.
103 An attack that tricks an email user into providing their confidential information or downloading malware through a hyperlink.
104 TM Venthan 'Cybersecurity in Lesotho: Current Challenges and Future Opportunities' (2023) 1 *Engineering Open Access* 129-141.
105 As above.
106 Unauthorised access to data or installation of spyware into a computer system. The software that takes over a computer system, corrupts data or conducts other malicious activities such as giving a malicious person access to personal information and financial accounts of the device.
107 The act of targeting an information system and encrypting its data, then demanding ransom to decrypt it.
108 Man in the Middle attack intercepts communication between two people and changes the contents of the communication messages.
109 Where an attacker takes over devices of a certain target and causes them to crash.
110 'Malicious and nuisance cyberattacks worry Lesotho' *Maseru Metro* 29 February 2020 https://www.maserumetro.com/news/business/malicious-and-nuisance-cyberattacks-worry-lesotho/ (accessed 02 August 2023).
111 Venthan (n 104).
112 Cavelty & Kavanagh (n 92) 78.
113 Ventham (n 104) & Maseru Metro (n 110).

Lesotho's legislative framework regarding cybersecurity is primarily addressed through the ICT Policy,[114] Data Protection Act (DPA), and Communications Act, albeit in a limited capacity. The ICT Policy emphasises the creation of a legal framework that offers "data protection and online security without unduly restricting access to information."[115] Under the DPA, data controllers or agents processing personal information are mandated to implement security measures to safeguard against loss or unauthorised access.[116] In the event of a data breach, controllers are required to notify affected individuals or the Data Protection Commission, which has the authority to disclose the identity of responsible parties for the protection of data subjects.[117] On the other hand, the Communications Act establishes legal safeguards against malicious activities within communication networks. It criminalises intentional damage of communication facilities belonging to another and the unauthorised alteration of message content sent on a communication service.[118]

To address cybersecurity concerns, Lesotho has a Computer Crime and Cybersecurity Bill in place.[119] The Bill extensively deals with cybersecurity and provides definitions[120] and strategic management of cybersecurity.[121] The Bill further provides for the protection of critical information infrastructure and regulation of cyber security incident management. It establishes a National Cyber Security Incident Response Team tasked with providing technical support to law enforcement agencies, implementing proactive and reactive measures to thwart cyber threats, enhancing public awareness of cybersecurity, and enhancing the expertise and capabilities of Lesotho's cyber workforce. It also provides for international cooperation in tackling cybersecurity issues.[122]

Additionally, the Bill introduces stringent measures to address cyber threats, categorising various actions as criminal offences against cybersecurity. These include illegally remaining in a computer system, illegal interference and interception of a computer system or data, illegal system interference that inhibits the proper functioning of a computer, data espionage, misuse of devices and software, cybersquatting, and social engineering attacks.[123]

The Bill presents a commendable strategy for tackling cybersecurity vulnerabilities that place Lesotho at risk of cyber attacks. It aligns with the principles outlined in the Malabo Convention, safeguarding privacy rights and enforcing crucial cybersecurity measures. Lesotho is actively also addressing cybersecurity concerns by promoting awareness among the public and regulatory entities. This proactive approach is evidenced by initiatives such as the cybersecurity symposium held in 2020[124] and the Cyber Security Summit in 2022.[125]

114 Minister of Communications, Science and Technology 'ICT Policy for Lesotho' (2005) https://ictpolicyafrica.org/en/document/nwx7t9x77bi (accessed 14 August 2023).
115 Minister of Communications, Science and Technology (n 114) 33.
116 Section 20 & 22 of DPA.
117 Section 23 of Data Protection Act.
118 Section 44 (e) & (g) of Communications Act.
119 Computer Crime and Cybersecurity Bill 2023.
120 Section 2 of Computer Crime Bill.
121 Part II Computer Crime Bill.
122 Section 12 of Computer Crime Bill.
123 Part II Computer Crime Bill.
124 Maseru Metro (n 110).
125 Lehaha Institute and the Governance Institute for Sustainable Development hosted this. https://cybersecuritylesotho.org/ (accessed 31 July 2023).

4.2 Cybercrimes legislation

Cybercrime is the use of computer systems, network devices or the internet to carry out criminal activities such as computer fraud or forgery.[126] The cybercrime law provides a framework for tackling cybercrimes. It defines conduct that should be criminalised and provides the procedure for investigation and prosecution.[127]

The Convention on Cybercrime of the Council of Europe 2001 (known as the Budapest Convention)[128] requires that while regulating cybercrime, states should strike a balance between law enforcement and protection of human rights enshrined in the ICCPR including freedom of expression, right to privacy and right of access to information.[129] The Budapest Convention is the first international treaty to deal with crimes committed on the internet.[130] It is aimed at establishing a common policy that targets the protection of society from cybercrimes by adopting legislation and promoting international cooperation.[131] It criminalises, amongst others, computer-related forgery and fraud, violations of computer networks and child pornography, now referred to as Child Sexual Abuse Material (CSAM).[132] The Budapest Convention further provides for procedures for the investigation of the crimes. For example, it sets out a procedure for the search of computer networks, real-time collection of traffic data and lawful interception.[133] The Malabo Convention deals with computer crimes as well. Article 25(1) mandates state parties to adopt legislative measures that criminalise acts that compromise the integrity, confidentiality, and availability of information and ICT systems.

Although Lesotho is not a state party of the two international instruments, it has taken steps to deal with cybercrimes through enactment of the Penal Code Act[134] and the Communications Act. The Penal Code criminalises unlawful access and or interfere with another person's computer or electronic storage device.[135] Similarly, the Communications Act makes it an offence to intentionally damage the communication facilities of another.[136]

The Computer Crime and Cyber Security Bill 2022 also provides for offences relating to the misuse of e-communication devices and networks (computer crimes), and establishes protocols for their investigation. The offences include illegal access, data espionage, computer-related forgery or forgery, child pornography, identity-related crimes, publication of false information,

126 Britannica 'Cybercrime' https://www.britannica.com/topic/cybercrime (accessed 02 June 2023).
127 Cavelty & Kavanagh (n 92) 97.
128 Council of Europe 'The Budapest convention (ETS No. 185) and its protocols' https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 12 May 2023).
129 According to Allison, The UN is considering developing a cybercrime treaty which will be an alternative to the Budapest Convention. Net Politics 'A New UN Cybercrime Treaty? The way forward for supporters of an Open, Free, and Secure Internet' *Council on Foreign Relations* 13 January 2020 https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet (accessed 12 May 2023).
130 Council of Europe 'Impact of the European convention on human rights' https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/ (accessed 12 May 2023).
131 Preamble of Convention on Cybercrime.
132 It further defines offences of illegal access, illegal interception, data interference, system interference, misuse of devices, offences related to child pornography, and offences related to copyright and related rights. It also lays down procedures on partial disclosure of traffic data, production order, seizure of computer data and real-time collection of traffic data, See Articles 16 to 21 of the Convention on Cybercrimes.
133 Article 19, 20 & 21 of Convention on Cybercrime.
134 Penal Code Act 6 of 2010.
135 Section 62 (2) of Penal Code.
136 Section 44 (1) (g) of Communications Act.

or any offence committed using a computer system or electronic form.[137] By enacting such legislation, Lesotho aligns with the standards set out in the Conventions.

Nonetheless, the first challenge identified in the Bill relates to its definition of illegal access and its effect on human rights. It provides that '[a] person who intentionally without lawful excuse accesses the whole or any part of a computer system commits an offence.'[138] Although the crime is defined in terms of 'intention' and 'without lawful excuse', the issue is that it is vaguely defined such that it may be abused or misused to criminalise acts of whistle-blowing or limit the media's freedom to access information. The Bill does not define 'without lawful excuse.' Lawful excuse presupposes authorisation. The absence of a clear definition limits whistle-blowers from imparting information. It also limits the media's freedom to access information, in that the media may source its information from the internet or from information that is in the public domain. The media's conduct may be deemed illegal if it does not constantly provide a justifiable reason for their sourcing of the data.

The second challenge is that the Bill criminalises publication of false information,[139] potentially encroaching into the realm of freedom of expression. The offence is defined as an act of publishing data that is false, misleading or deceptive, with the intention to mislead or deceive the public. Such a provision may create a chilling effect, causing individuals and media outlets to hesitate in expressing their opinions or sharing information for fear of being deemed deceptive and facing legal repercussions. In this regard, the Bill falls short in safeguarding digital rights.

While the Bill is commended for criminalising cyberterrorism, concerns arise due to the overly broad definition of the offence, potentially infringing on some human rights. By criminalising cyber terrorism, Lesotho aligns with the OAU Convention on the Prevention and Combating of Terrorism[140] and its Protocol,[141] in that it acknowledges that terrorists may use sophisticated technologies and communication systems to commit acts of terrorism. However, the Bill's definition of cyberterrorism extends to the communication of information that destabilise political, economic and social structures of a country or international organisation.[142] The definition is vague as it labels legitimate political opposition, advocacies, protests, demonstrations or industrial actions, as acts of terrorism. Such ambiguity undermines peoples' right to seek, receive and impart information and ideas, right to free flow of information, right to freedom of expression and opinion on any medium of communication, and ultimately stifles the right to political participation and freedom of association. In contrast, Lesotho's Prevention and Suppression of Terrorism Act 3 of 2018 prudently excludes activities that fall within the realm of freedom of expression from being classified as acts of terrorism.[143]

137 Part IV Computer Crime Bill.
138 Section 21 (1) of Computer Crime Bill.
139 Section 43 of Computer Crime Bill.
140 Organisation of African Unity 'Convention on the Prevention and Combating of Terrorism' (1999)37289-treaty-0020_-_oau_convention_on_the_prevention_and_combating_of_terrorism_e.pdf (accessed 12 September 2023).
141 Protocol to the OAU Convention on the Prevention and Combating of Terrorism, 01 July 2004 37291-treaty-0030_-_protocol_to_the_oau_convention_on_the_prevention_and_combating_of_terrorism_e.pdf (accessed 12 September 2023).
142 Section 27 of Computer Crime Bill.
143 Section 2 Prevention and Suppression of Terrorism Act 3 of 2018 https://media.lesotholii.org/files/legislation/akn-ls-act-2018-3-eng-2018-01-26.pdf (accessed 12 September 2023).

Moreover, the Bill's definition of illegal data interference discourages whistle-blowing. It renders the intentional interference with the lawful use of a computer without lawful excuse, or the communication, disclosure or transmission of computer data to a person who is not authorised to access the data, an offence. The act of receiving computer data without authorisation is an offence as well.[144] The definitions of illegal data interference, deter whistle-blowers from disclosing useful information to the benefit of the society for fear of being charged with an offence. Consequently, the Bill undermines fundamental rights such as the freedom to seek, receive, and disseminate information, as well as the right of access to information.

The criminalisation of unsolicited messages also undermines the right to assemble, freedom of association, free flow of information and political participation to a certain extent. The Bill makes it an offence to use a computer to share multiple communications which are misleading or deceiving.[145] This discourages an association of persons with similar ideological, political, cultural or social interests from mobilising movements that oppose government or organising structures, and threatens their right to political participation.

Although the offence of data espionage protects the confidentiality of information and ensures cybersecurity,[146] it may inadvertently limit the right to access information which is crucial in citizen's participation in their government. This right is indispensable for informing decisions related to political, economic, and social reforms, thereby hindering the potential for meaningful societal change.

The Malabo Convention requires states to establish procedures for the prosecution of criminal offenders, ensuring these procedures adhere to human rights standards, especially those outlined in the African Charter.[147] The commendable aspect of the Bill lies in its procedural law requirement for enforcement officers to obtain a court order before conducting search and seizure on computer systems or data which may be evidence in criminal investigations.[148] However, a cause for concern arises from the provision permitting legal officers to extend the scope of the court order to seizure of computer systems or data not initially covered by the order, based solely on suspicion of potential relevance to the investigation.[149] This lack of sufficient safeguards raises apprehensions about potential abuses of power. Such provisions risk facilitating arbitrary searches and seizures, directly contravening the principles enshrined in the Constitution.[150]

The preceding discussion reflects attempts by Lesotho to address computer crimes through the drafting of the Computer Crime and Cyber Security Bill.[151] However, the Bill has the potential to undermine critical digital rights including the right to assemble, freedom to associate, access to information, freedom of expression and freedom from arbitrary search and seizure. To this extent, regrettably, the Bill does not strike a balance between the protection and promotion of digital rights and the limitation of the rights for national security purposes as set out by

144 Section 24 (1) (b) & (2) (a) &(c) of Computer Crime Bill.
145 Section 38 of Computer Crime Bill.
146 Section 26 of Computer Crime Bill.
147 Article 25 (1)-(3) of AU Convention on Cyber Security and Personal Data Protection.
148 Section 59 (1) of Computer Crime Bill.
149 Section 59 (2) of Computer Crime Bill.
150 Sections 10 & 17 of the Constitution.
151 Pule (n 83) 6. It is noted that the first draft of the Bill was rejected by the National Assembly for lack of sufficient consultation with stakeholders such as the Transformation Resource Centre (TRC) and MISA Lesotho, contrary to Section 20 of the Constitution and Article 13 of the ACHPR that allow every citizen the right to participate in government.

the Constitution. The Bill's limitations are not in the interests of public defence of safety. The following recommendations are proposed to address the shortcomings of the Bill and ensure the realisation of digital rights.

Recommendations

It is recommended that the Ministry of Communications, Science and Technology revise the Bill as follows:

- Align the offence of illegal access with international standards, such as those outlined in the Budapest Convention on Cybercrime. For instance, an individual commits illegal access when they breach security measures with the intent of obtaining computer data or engaging in dishonest activities, or when they interfere with a computer system connected to another system.[152] Alternatively, consider refraining from criminalising illegal access altogether.

- Refine the definition of cyber terrorism to exclude the communication of information intended to destabilise political, economic, and social structures within a country or organisation.

- Clarify the definition of illegal data interference to specifically exclude actions that interfere with the lawful use of a computer or involve the unauthorised reception of computer data.

- Avoid criminalising the act of sharing multiple communications through a computer that may potentially mislead or deceive, unless they qualify as unsolicited messages in a broader context.

- Ensure that law enforcement officers are required to obtain an extension of a court order from the appropriate judicial authority before conducting searches and seizures that extend beyond the scope of the original court order.

4.3 Data protection and the right to privacy

The right to privacy is guaranteed and protected under international human rights laws and standards.[153] The ACHPR 2019 Declaration guarantees the right to privacy,[154] which includes the confidentiality of communications and protection of personal information on the internet.[155] To facilitate upholding these rights, the Declaration requires states to adopt legal frameworks aligning with international human rights law and standards, taking into account the principles of legality, fairness, transparency and confidentiality, while prioritising the pertinent requirement of consent from data subjects before any processing occurs. They should also restrict information processing solely to its intended purpose, forbidding indiscriminate collection, storage, or dissemination. The Declaration also enshrines the rights of data subjects, granting them access to their processed personal data, empowering them to rectify inaccuracies or

152 Article 2 of Convention on Cybercrime.
153 'No one shall be subjected to arbitrary interference with his privacy'. Article 12 UDHR and Article 17 (1) ICCPR.
154 Declaration on Principles of Freedom of Expression and Access to Information in Africa in 2002 and revised in 2019.
155 Principles 40 (1) & (2) ACHPR 2019 Declaration.

omissions, and enabling them to object to any processing deemed intrusive. It also mandates timely notification in cases of unauthorised access to personal information. Recognising the detrimental impact of sharing harmful personal data, such as intimate images or child sexual abuse material, the Declaration mandates criminalisation and establishes avenues for effective legal redress. Complementing these provisions, states should institute robust oversight mechanisms, endowed with the requisite expertise in human rights and privacy, to ensure effective data protection and privacy rights enforcement.[156]

Similarly, the Malabo Convention sets out six basic principles on data processing to safeguard data protection. These are confidentiality and security; consent and legitimacy; lawfulness and fairness; purpose, relevance and storage of processed personal data; accuracy of personal data; and transparency.[157] The Convention mandates that each state should establish a national Data Protection Authority (DPA) tasked with the responsibility of ensuring adherence to the aforementioned data processing principles.[158] The SADC Model Law on Data Protection 2013 enshrines similar principles.

Lesotho has initiated efforts that contribute to data protection. The Constitution provides for the right to respect private and family life.[159] According to *Kali v Mahasele*[160] 'private life' is, of course, a reference to the right to privacy.' Thus, a right to privacy is deduced from the right to private and family life. Correspondingly, the court in *Mofomobe and Shale v the Prime Minister and 2 Others* stated that Section 11 of the Constitution protects the right to privacy.[161] It is noted that the right to privacy is extended to data protection as encapsulated by the ACHPR 2019 Declaration. The right to privacy may only be limited in the interests of defence, public order or for protection of other peoples' freedom.[162]

In addition to the Constitution, Lesotho enacted the Data Protection Act[163] (DPA) to regulate the processing of personal information and to protect its privacy. Section 2 of DPA defines processing as an operation or activity relating to the collection, receipt, recording, collation, organisation, storage, modification, retrieval, consultation or use of information. The definition extends to the dissemination of information, or merging, linking, blocking, degrading, erasure, or destruction of information.

Section 15 (2) of DPA provides circumstances under which personal information shall be processed. These include instances where the data subject provides explicit consent to the processing; where processing is necessary for compliance with a legal obligation to which the data controller is subject; where the processing is intended to protect the legitimate interests of the data subject; or for the proper execution of a public law duty by a public body. In adherence to this provision, a data controller is mandated to cease processing a data subject's personal data upon the Data Protection Commission's validation of the data subject's objection to such processing.[164]

156 Principle 41 (1) & 42 (1) - (8) ACHPR 2019 Declaration.
157 Article 13 of AU Convention on Cyber Security and Personal Data Protection.
158 Article 11 of AU Convention on Cyber Security and Personal Data Protection.
159 Section 11 (1) of Constitution.
160 *Kali v Mahasele* (C of A (CIV) 19 of 2011) [2011] LSCA 27 (21 October 2011) https://old.lesotholii.org/ls/judgment/court-appeal/2011/27 (accessed 02 May 2023) .
161 *Mofomobe and Shale v. The Prime Minister and others* [2023] LSHC 125 Cons, para 14.
162 Section 11 (2) Constitution.
163 Data Protection Act 5 of 2011 https://ictpolicyafrica.org/en/document/i6dvu4pq63 (accessed 03 September 2023).
164 Section 15 & 39 of the DPA.

Further, DPA establishes essential safeguards for data processing. It provides that personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.[165] It also mandates that personal data should be collected for specific, clearly stated purposes, and not used for any other Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes.[166] The DPA also imposes a duty on data collectors to safeguard personal information, ensuring it remains protected from unlawful access, loss, or damage, while maintaining its integrity.[167]

The DPA also specifies that personal information should ideally be collected directly from the individual, with a few exceptions. It may not be collected from the data subject if: the information is in the public domain; the data subject has consented to the collection of the information from another source, or it would not prejudice the data subject; it is for enforcement of law and order; it is in the interests of national security or; collection from the data subject would prejudice a lawful purpose of the collection.[168]

Otherwise, it is incumbent upon the data controller to inform the data subject about the collection of their information and its intended purpose.[169] The data controller should also take reasonable steps to ensure that the information is complete, accurate, not misleading and up to date.[170] Should there be any doubts regarding the accuracy of the gathered data, the data subject reserves the right to contest it and request the data controller to rectify any inaccuracies, incompleteness, misleading aspects, or outdated information.[171] They also have a right to request the data controller to delete the information if they no longer have a right to retain it.[172]

A data controller is prohibited from transferring personal information concerning a data subject to a third party located in a foreign country without the explicit consent of the data subject.[173] The DPA extends its protections by prohibiting the processing of sensitive personal information, including data related to children without parental consent, as well as information pertaining to religious beliefs, sexual orientation, racial identity, political affiliations, or criminal history, among others.[174] In cases where there is reason to suspect that collected information has been accessed by an unauthorised entity, it is mandatory for the data controller to promptly notify both the affected data subject and the Data Protection Commission.[175]

The DPA establishes the Data Protection Commission, tasked with a broad mandate including promoting education and public awareness of information protection principles, monitoring and enforcing compliance with the Act's provisions, and monitoring technological advancements to minimise adverse effects on personal data.[176] A data subject may report breaches of the DPA with the Commission, which has the authority to conduct investigations.[177] The Commission is

165 Section 16 of DPA.
166 Section 18 (1) of DPA.
167 Section 20 of DPA.
168 Section 17 of DPA.
169 Section 25 of DPA.
170 Section 24 (1) of DPA.
171 Section 27 (1) (a) of DPA.
172 Section 27 of DPA.
173 Section 52 (b) of DPA
174 Section 29 of DPA.
175 Section 23 (1) of DPA.
176 Section 6 & 8 of the DPA.
177 Section 39 of DPA.

empowered, where appropriate, to act as a conciliator to facilitate dialogue between involved parties to facilitate settlements, and issue enforcement notices mandating data controllers to cease specific data processing activities.[178] However, despite the Act's enactment, the Commission has not yet been established, leaving a void in compliance monitoring.[179] Nonetheless, a data subject may institute a civil action for damages against data controllers in courts with appropriate jurisdiction.[180] Although the DPA complies with international human rights laws and standards such as principles 40 and 42 of the ACHPR 2019 Declaration, the failure to establish an oversight mechanism to monitor its implementation undermines the realisation of the benefits and rights outlined in the legislation.

There are legal instruments in Lesotho which permit data processing, without explicit consent of a data subject contrary to human rights standards. The Communications (Subscriber Identity Module Registration) Regulation (Communications Regulation) grants authorisation to licence holders (VCL and Econet) to capture, register and retain personal information of sim card subscribers.[181] Licensees can work with the National Identity and Civil Registry to verify the authenticity of the subscribers' identity cards.[182] Licensees are empowered to deactivate unregistered SIM cards or withhold activation of new ones until subscribers register their personal details, rendering the collection of such data mandatory.[183][184] However, this practice of collecting personal information without explicit consent violates the data protection safeguards enshrined in relevant legal instruments. The Communications Regulation is therefore not in conformity with international human rights law and standards on the protection of the digital right to privacy.[185]

The Communications Regulation's imposition of mandatory data processing encroaches on the right to privacy without sufficient constitutional justification.[186] In terms of the Oakes test,[187] which assesses whether a law that restricts a constitutional right is justified, several criteria should be met: the law's objective should be clearly articulated, pressing, and substantial; it should be logically connected to this objective; demonstrate that the law minimally impairs the right in question; and the benefits derived from the law should outweigh its negative impact on the limited right. Failure to meet any of these criteria renders the limitation unjustified and unconstitutional. The objective of the Communications Regulation is to provide a regulatory framework for SIM card registration. However, the regulation falls short in justifying the significance of this framework, thus failing to demonstrate a pressing and substantial objective. Thus, it becomes challenging to assess whether the benefits of the law outweigh its encroachment on the right to privacy, as the objective is vague. Accordingly, the Communications Regulation fails to pass the Oakes test's requirements for justifying such limitations on constitutional rights.

178 Section 40 & 46 of the DPA.
179 Pule (n 83) 7.
180 Section 49 of DPA.
181 Regulation 7 of Communications (Subscriber Identity Module Registration) Regulation.
182 IK Kassouwi 'Sim card registration to begin in Lesotho next June 24' Ecofin Agency 21 May 2022 https://www.ecofinagency.com/telecom/2105-43612-sim-card-registration-to-begin-in-lesotho-next-june-24 (accessed 26 May 2023).
183 Regulation 9 (2) of Communications Regulation.
184 Regulation 17 (1) of Communications Regulation.
185 See for example Principle 40-42 of ACHPR 2019 Declaration; Article 12 of the UDHR and article 17 (1) of the ICCPR.
186 Section 11 (2) of Constitution.
187 *R v Oakes*, 1986 1 SCR 103 is a Canadian Supreme Court case that established a test for determining whether a law that infringes a right is justified. Lesotho adopted the Oakes test through the case of *Attorney General of Lesotho v Mopa* LAC (2000-2004). See *Mofomobe* Case (n 166) para 16 for further guidance on the restrictions of the right to privacy.

The Prevention of Corruption and Economic Offences Act also authorises data processing without the consent of a data subject.[188] It authorises a Director of Prevention of Corruption and Economic Offences to compel individuals to disclose information relating to a suspect during investigations into an offence, without the consent of the suspect's consent.[189] This provision,

though potentially infringing upon the privacy of the data subject, is deemed justified as it serves the broader interest of public order, as sanctioned by constitutional provisions.[190]

In recognition of the right to privacy, the Broadcasting Code, states that a broadcaster should not present information that violates a person's privacy and family life unless it is in the public interest to do so.[191] The Code protects the right to privacy and its restrictions of the right fall within the constitutional law limitations of the right.[192] It therefore observes human rights standards.

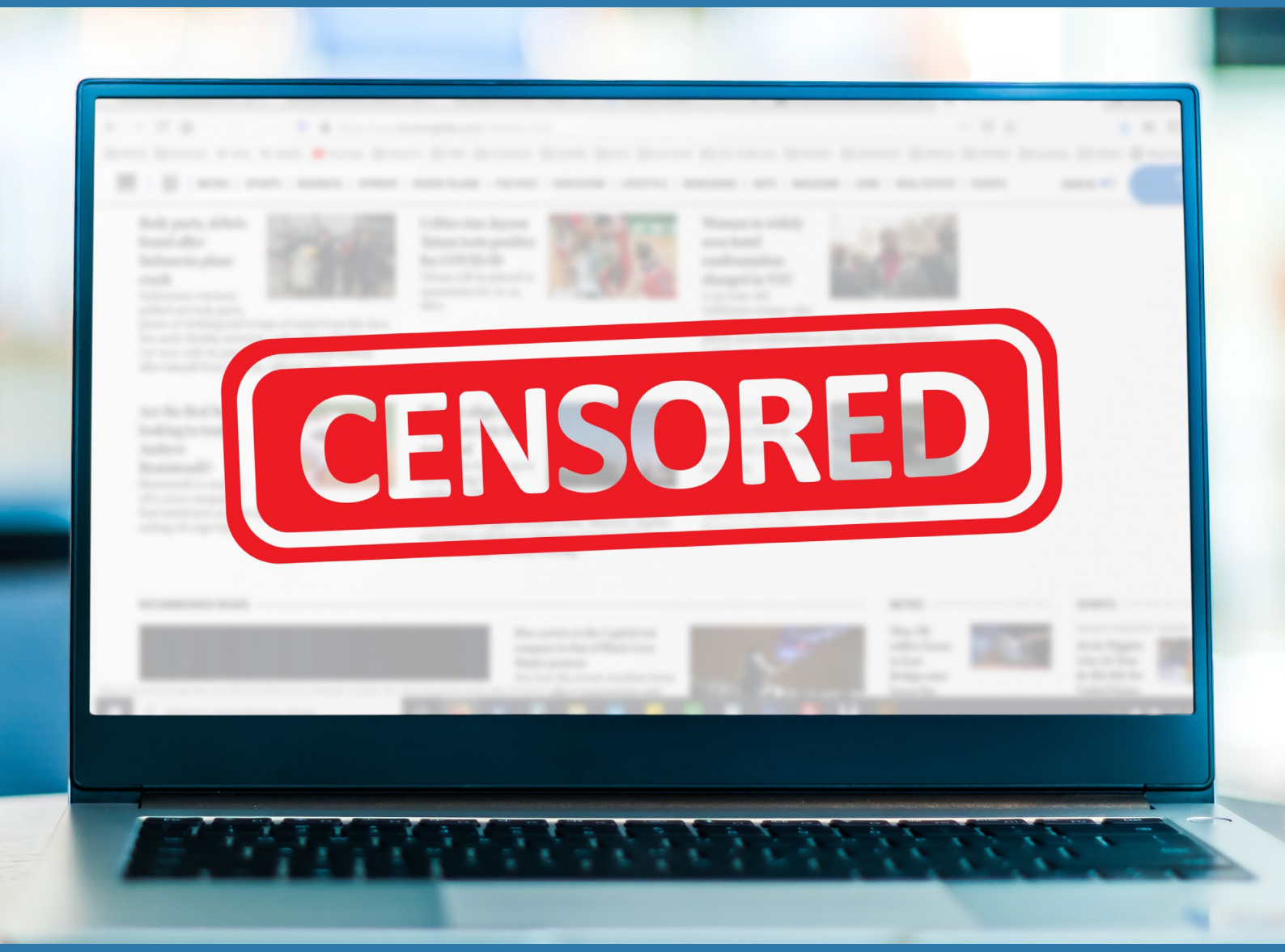
Regarding anonymity, the ACHPR 2019 Declaration spotlights the importance of anonymity in online communication, affirming individuals' right to use pseudonyms or communicate anonymously to safeguard their identity and communications. Technologies like Virtual Private Networks (VPNs) and onion routers are highlighted as viable means to ensure anonymous communication. It explicitly cautions against any state actions that compromise encryption technologies, emphasising that such measures should only be considered if they align with international human rights standards. However, the Computer Crime and Cyber Security Bill in Lesotho takes a contradictory stance by criminalising unsolicited messages, including those transmitted via electronic devices that conceal message origins. Despite this, the Bill lacks substantive justification for this provision, thereby violating individuals' right to privacy.

Recommendations

The following recommendations are proposed to enhance privacy protection and align regulatory frameworks with international standards:

- The Ministry of Communications, Science and Technology should expedite the establishment of the Data Protection Commission to ensure the effective observation, monitoring, and enforcement of privacy principles.
- The Ministry of Communications, Science and Technology should amend the Communications Regulation to either justify its limitation of the right to privacy by mandatory processing of data or delete sections that render the processing of data mandatory.
- The Ministry of Communication, Science and Technology should amend the Computer Crime and Cyber Security Bill by revising the definition of unsolicited messages to prevent the unintended prohibition of technologies that preserve the anonymity of information sources on the internet.

188 Prevention of Corruption and Economic Offences Act 5 of 1999.
189 Section 8 (1) (b) - (d) of Prevention of Corruption and Economic Offences Act.
190 Section 11 (2) (a) of the Constitution.
191 Section 11 (1) (a) of the Broadcasting Code.
192 Section 11 (2) the Constitution.



CHAPTER 5

FREEDOM OF EXPRESSION ONLINE AND ACCESS TO INFORMATION IN THE DIGITAL AGE

5. FREEDOM OF EXPRESSION ONLINE AND ACCESS TO INFORMATION IN THE DIGITAL AGE

Digital rights find expression across diverse media channels, including television, radio, print, and digital platforms like websites, applications, and social media networks.[193] This section explores the role of the media in the context of digital rights, including the constraints that may undermine their exercise.

5.1 The role of the media in the context of digital rights

The media bears an important responsibility to both inform and educate the public. Its role extends beyond mere dissemination to vigilant oversight, particularly concerning those in positions of authority—be it within the government, public offices, or the private sector.[194] By monitoring and reporting on their actions, the media serves as a vital watchdog, illuminating matters that directly and indirectly impact the public. For instance, the broadcast of Parliament Public Accounts Committee proceedings in 2019 offered insight into the activities of public officials.[195] In championing accountability, fairness, and transparency, the media becomes an advocate for good governance and democracy, nurturing a more informed and engaged citizenry.[196]

To effectively fulfil this mandate, states should safeguard media freedom, ensuring free flow of information and ideas. This includes the right of access to information and the fundamental principle of media freedom, which is an integral part of freedom of expression. The Windhoek Declaration reiterates this, citing article 19 of the UDHR,[197] which emphasises the importance of establishing and 'maintenance of an independent, pluralistic and free press is essential to the development and maintenance of democracy in a nation, and for economic development.'[198] It is therefore the responsibility of states to guarantee press independence, shielding it from political, governmental, or economic influence. They should also eliminate monopolies and create an environment that promotes diverse media landscapes, promoting a diversity of voices and perspectives.[199]

The ACHPR 2019 Declaration guarantees freedoms relevant to the media in the digital age.[200] It mandates states to protect freedom of expression and access to information both offline and online.[201] Aligned with the Windhoek Declaration, it asserts that media monopoly stifles freedom of expression and encourages states to promote pluralistic media.[202] The Declaration further provides that states should guarantee media independence, including print, broadcast

193 J Limpitlaw 'Media Law Handbook for Southern Africa' (2021) 8, 10 mlhsa-2021-volume-2-ebook (accessed 15 September 2023).
194 Such as current affairs, general education matters, economic development activities, entertainment and sports.
195 MISA Zimbabwe 'The State of Press Freedom in Southern Africa (2019-2020)'(2020)12.
196 Centre for Human Rights (n 2) 45.
197 It guarantees freedom of expression as a basic human right and promotes the free flow of information and ideas.
198 MISA 'Windhoek Declarations on Promoting Independent and Pluralistic Media' (1991) https://misa.org/wp-content/uploads/2015/06/Windhoek-Declaration.pdf (accessed on 29 July 2023).
199 MISA (n 198) 2-3.
200 The ACHPR 2019 Declaration is an expansion of rights in Article 9 of the African Charter, Article 19 UDHR, and Article 19 ICCPR.
201 Principle 5,6 & 37 ACHPR 2019 Declaration.
202 Principle 11 ACHPR 2019 Declaration .

and online media.[203] The declaration advocates for the establishment of independent regulatory bodies to oversee broadcast, communications, and internet infrastructure, shielding them from political influence.[204] Crucially, it mandates states to safeguard journalists from undue legal constraints and physical harm, ensuring their safety amidst an array of potential threats including intimidation, kidnappings, unlawful surveillance, killings or other forms of ill-treatment by state or non-state actors, and take effective measures to punish perpetrators of the attacks.[205] Upholding the principles of net neutrality, it calls upon states to compel internet intermediaries to facilitate unrestricted internet traffic.[206] Additionally, it acknowledges the right of journalists to organise and advocate for their own protection and rights.[207] The Declaration offers a comprehensive framework for states to advance and safeguard digital rights, through the prism of media freedom.

In advancing media freedom, Lesotho has adopted legislation and other regulatory instruments that guarantee these fundamental rights. Firstly, section 14 of the Constitution provides that every person is entitled to freedom of expression and opinion and to receive and communicate information and ideas. Section 13 enshrines the freedom of conscience, including the right to freedom of thought. This provision empowers journalists to fearlessly engage with critical public issues, fortified by the assurance of protection from undue interference.[208] Thirdly, Section 10 guarantees freedom from arbitrary search and entry, shielding journalists' materials such as notebooks and digital storage devices from unwarranted intrusion.[209][210] This safeguard extends to safeguarding the confidentiality of journalists' sources and informants, ensuring the integrity of investigative journalism.[211] The Constitution also provides for the right to life, the right to personal freedom, freedom of movement, and freedom from inhuman treatment.[212] Beyond these constitutional guarantees, Lesotho's legal framework includes a range of other essential rights, including the right to life, personal freedom, freedom of movement, and protection from inhuman treatment. The Constitution also explicitly recognises the freedom of association, ensuring that individuals, including media practitioners, can assemble and collaborate for common ideological pursuits without hindrance.[213] Complementing these constitutional provisions, the Penal Code imposes penalties for offences against media integrity, serving as a deterrent against infringements on press freedom.[214] Collectively, these legal safeguards serve as pillars underpinning the vitality of Lesotho's media landscape, both in traditional and digital spheres, creating an environment conducive to robust journalism and public discourse.

Despite the basic rights guaranteed above, there are laws in Lesotho that limit the freedom of expression of the media. For instance, the Printing and Publishing Act criminalises the

203 Principle 12 (1) of ACHPR 2019 Declaration.
204 Principle 17 of ACHPR 2019 Declaration.
205 Principle 20 of ACHPR 2019 Declaration . Media violations extend to threats of journalists; attacks of media outlets, arbitrary search of media outlets, closing them by force, confiscation of equipment; inability to broadcast or report due to shut down of online sites; arbitrary search of media and legislation that inhibit media to report freely and fearlessly.
206 Principle 39 of ACHPR 2019 Declaration .
207 Principle 19 of ACHPR 2019 Declaration .
208 Limpitlaw (n 193)7.
209 Section 10 (1) Constitution: 'Every person shall be entitled to freedom from arbitrary search or entry, that is to say, he shall not (except with his own consent) be subjected to the search of his person or his property or the entry by others on his premises.'
210 Section 17 Constitution.
211 Limpitlaw (n 193) 5, 7.
212 Chapter II of the Constitution.
213 Section 16 (1) of Constitution.
214 Part III of Penal Code.

dissemination of content deemed hazardous to public safety or order.[215] Similarly, the Internal Security (General) Act prohibits publications that could incite public violence,[216] while also restricting media access to protected areas, hindering their ability to report on pertinent activities.[217] The Sedition Proclamation[218] penalises the publication of material deemed seditious, with an overly broad definition that is inclusive of expressions of dissent or discord against the government or among societal groups.[219] Moreover, the Penal Code Act criminalises the publication of information likely to incite public violence.[220] These legislative measures severely curtail the media's capacity to fulfil its watchdog function and promote democracy, both in digital spaces and traditional media platforms.

While international standards[221] uphold the media's right to access information, Lesotho lacks specific legislation to guarantee this right. The Lesotho Law Reform Commission drafted the Access and Receipt of Information Bill in 2000, aiming to facilitate access to information. But the Bill was never passed in parliament. Unfortunately, this crucial bill never made it through parliament, leaving the media in a precarious position when it comes to requesting and obtaining information from public entities.[222] Adding to the challenge, certain laws actively inhibit public officials from sharing information, effectively stifling criticism of governmental bodies.[223] For instance, there are laws that impose information restrictions on officials within their respective domains. The Official Secrets Act of 1967 prohibits civil servants from disclosing information.[224] The Prisons Proclamation 1957 makes it an offence for an official to communicate to the press about information they came across while executing their duties, or to publish information about prison services.[225] Similarly, the Police Service Act prohibits police officers from disclosing information pertaining to their duties unless mandated by a court of law or within the scope of their official responsibilities.[226] These legislative barriers not only hinder transparency but also impede the media's ability to fulfil its watchdog role.

The media's vital role in informing the public is severely hindered by the significant lack of access to information in Lesotho, as highlighted by a transparency study conducted in 2020. Shockingly, over 70% of both public and government institutions in the country denied access to crucial information, while only 30% offered open access.[227] This glaring disparity severely undermines the media's ability to fulfil its duty to keep the public informed. Regrettably, Lesotho falls short of meeting the standards outlined in the Model Law on Access to Information for Africa, which enshrines every individual's right to request information from public entities.[228]Information officers may refuse to provide the information where doing so would be prejudicial to national security or defence.[229] The African Platform on Access to Information emphasises governments'

215 Section 20 (1) of Printing and Publishing Act 1967.
216 Section 34 Internal Security (General) Act 1984.
217 Section 38 Internal Security (General) Act 1984.
218 Sedition Proclamation 44 of 1938
219 Limpitlaw (n 193) 316.
220 Section 85 of Penal Code Act.
221 Article 19 UDHR, Article 9 African Charter; Article 4 ACHPR 2019 Declaration.
222 MISA Lesotho 'Promoting free expression in Southern Africa' https://lesotho.misa.org/issues-we-address/media-freedom-monitoring/ (accessed 02 August 2023).
223 UNCHR 'Freedom of the press 2015 – Lesotho' https://www.refworld.org/docid/56531356c.html (accessed 19 May 2023).
224 Section 4 of Official Secrets Act.
225 Section 156 of Prison Proclamation.
226 Section 27 of Police Service Act.
227 MISA 'The state of press freedom in Southern Africa (2019-2020)' 12.
228 Article 12 of ACHPR Model law.
229 Article 30 ACHPR Model Law .

obligation to leverage ICTs to ensure maximum transparency and disclosure of information.[230] Regarding media independence, the Lesotho Communications Authority (LCA), responsible for regulating broadcasting in the country, suffered a blow to its autonomy with the amendment of the Lesotho Communications Authority Act 5 of 2000 in 2006. The amendment deleted the words 'autonomous and independent' from the definition of the Authority, thus undermining its position.[231] Such a move directly contradicts the principles outlined in the Windhoek Declaration and Principle 12 of the ACHPR 2019 Declaration. Despite efforts made in the Constitution to safeguard freedom of expression and access to information in the digital age, including protections for media rights, it falls short of ensuring these rights as mandated by the ACHPR 2019 Declaration. The inadequacy of legal protections underlines the urgent need for Lesotho to address these deficiencies and uphold the fundamental rights of its citizens in the digital era.

Recommendations

In light of the aforementioned considerations, the following recommendations are proposed to promote media freedom in the digital age, so that it performs its mandate independently, freely and without fear.

- The Ministry of Communications, Science, and Technology should prioritise the revision and enactment of the Access and Receipt of Information Bill. This legislation will be crucial in guaranteeing both media outlets and citizens access to information, a fundamental cornerstone of media freedom in the digital age.
- The Ministry of Communications, Science and Technology should initiate the development of comprehensive policies aimed at safeguarding media freedom. These policies should be inclusive of various aspects such as protection of journalists, promoting an environment conducive to investigative journalism, and ensuring the independence of media institutions.
- The Ministry of Law and Constitutional Affairs should take proactive measures to develop legislation that explicitly prohibits infringements on media freedom.[232] This legislation should not only define what constitutes a violation but also establish mechanisms for the prosecution of perpetrators. Such legal frameworks should be aligned with international standards, particularly the ACHPR 2019 Declaration.
- The Ministry of Communication, Science and Technology should prioritise the independence and autonomy of regulatory bodies such as the LCA, through amendments to the relevant legislation. The LCA Act should be amended accordingly. A robust and independent regulatory framework is essential for safeguarding media freedom and ensuring that access to information remains uninfluenced by political agendas.

By implementing these recommendations, the public can effectively embrace the digital rights afforded by media freedom.

230 APAI (n 44) para 13.
231 Limpitlaw (n 193) 16.
232 'Media violations include: when journalists are physically or verbally assaulted, threatened, injured, kidnapped, disappear, arrested, killed, censored, denied credentials or wrongfully expelled during the course of their work or as a direct result of their work; when news outlets are attacked, illegally searched, censored, closed by force, raided, unable to report, broadcast or publish because of factors such as the confiscation of equipment, blocking of their online site or the jamming of transmissions; when new legislation or changes to legislation hinder journalists from conducting their work freely and without fear.' MISA Lesotho 'Media freedom monitoring' https://lesotho.misa.org/issues-we-address/media-freedom-monitoring/ (accessed 10 May 2023).

5.2 Media and civic space sustainability in the digital age

Civic space is a political, economic and legislative environment where individuals can freely converge to express their perspectives and advocate for their interests, thus actively contributing to the collective shaping of their communities.[233] Within this sphere, the public engage in dynamic interactions, unfettered by governmental, familial, or commercial constraints.[234] It serves as the crucible for collective action, where diverse voices coalesce to pursue shared objectives or challenge prevailing norms, whether through the collective strength of civil society organisations[235] and media outlets, or the courageous efforts of individual human rights defenders. Civic space plays an indispensable role in promoting good governance, particularly in advancing accountability, inclusivity, and social cohesion. [236]

In a civic space, civil societies fulfil vital democratic functions. First, they safeguard citizens' rights by vigilantly monitoring governmental actions and holding authorities accountable.[237] Through robust media and civil organisations, they serve as a bulwark against potential abuses of power or legal transgressions by the state, thereby curbing excessive government influence.[238] Secondly, civil societies serve as advocates and conduits of public communication. Through lobbying efforts and awareness campaigns on governance issues, they prioritise public needs and provide essential civic education, often through media releases. Disseminating crucial information empowers the public to pursue their interests effectively.[239] Thirdly, civil societies facilitate socialisation by providing platforms for citizens to engage in discussions on matters impacting their well-being.[240] Through open expression of opinions and collaborative problem-solving, they cultivate political participation[241] and facilitate constructive dialogue between governmental bodies and the public. Effective decision-making necessitates the inclusion of voices from the state, the public, and civil societies, underscoring the critical role of citizen participation in sustaining democracy.

States play a crucial role in promoting an open and dynamic civic space conducive to the effective operation of civil societies and individuals in carrying out their respective roles.[242] Central to this is the state's commitment to upholding civic freedoms. For one, the civic space will be open and vibrant if a state respects civic freedoms. A vibrant civic space hinges on the state's respect for fundamental rights, such as the right of access to and free flow of information, freedom of expression, freedom of association, freedom of assembly, and right to participation. This commitment necessitates the establishment of supportive legal frameworks, policies,

233 European Civic Forum 'Civic Space Watch' https://civic-forum.eu/civic-space (accessed 02 September).
234 A Buyse 'Squeezing civic space: restrictions on civil society organizations and the linkages with human rights' (2008) 22 *The International Journal of Human Rights* 966-988.
235 'A civil society is regarded as a public association that allows people with different values, ideas and different political party affiliations to come together for the common goal of ensuring that the government does not abuse its powers', with the believe that it will help the governance of the country' Unpublished: M Rakhare 'The impact of civil society on governance in Lesotho' unpublished PhD Thesis, University of Free State.
236 M Rakhare & T Coetzee 'The Impact of Civil Society on Governance in Lesotho' (2020)12 *Insight on Africa* https://doi.org/10.1177/0975087820909333 (accessed 02 October 2024).
237 T Roberts 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries' (2021).
238 M Kapa & L Theko 'The role and position of civil society organisations in Lesotho's democratisation process' 2008 7 *Journal of African Elections* 128.
239 As above.
240 Rakhare &Coetzee (n 236).
241 Kapa & Theko (n 238).
242 A political space in an environment in which governing institutions receive and consider the input of its citizens.

institutions, and practices geared towards safeguarding these rights. Effective implementation of such measures is paramount to ensuring the vitality and protection of civil societies. For instance, the state should extend protection to human rights activists and whistleblowers who expose malpractices within governing bodies, shielding them from reprisals or punitive actions. Thus, '[g]overning bodies have the duty to protect the civic space, refrain from, investigate and discipline actions, laws and statements that threat civic freedoms.'[243] Upholding these principles not only preserves the integrity of democratic institutions but also promotes an environment where civil societies can thrive and contribute meaningfully to societal progress. Additionally, a thriving civic space hinges on encouraging an ongoing dialogue between governing bodies and civil societies. States ought to devise strategies aimed at empowering citizens and civil societies to engage meaningfully and actively in public discourse and policy formulation.[244] Further, civil societies should have the capacity to respond to challenges to the rule of law, democracy and fundamental rights.[245] By embracing these principles, Lesotho can cultivate a dynamic and sustainable civic environment.

Public participation in the civic space may be conducted offline or online. In the online sphere, it is carried out on numerous platforms, including internet-based communication avenues like social media, online forums, email exchanges, and more. Within this online civic landscape, individuals assume diverse roles as bloggers, citizen journalists, commentators, human rights advocates, and creators of content on social networks.[246] Therefore, the internet stands out as a crucial catalyst for nurturing information democracy and enabling active participation by citizens in civic spaces.[247]

Several factors contribute to the evolution of digital spaces for civic engagement. Foremost among these is the provision of secure and private online communication facilitated by cutting-edge privacy-enhancing tools and technologies.[248] By employing digital security measures, individuals can encrypt their exchanges and maintain anonymity, effectively thwarting intrusive state surveillance. The broadening accessibility to digital platforms, whether through the widespread adoption of mobile phones or the facilitation of internet connectivity, serves as another cornerstone of digital empowerment. In tandem, the rise of social media activism manifests as a formidable influence, granting dissenting voices a platform for expression and amplifying their messages for broader consideration. Finally, legislative initiatives play a crucial role in shaping the digital landscape, particularly those aimed at safeguarding digital rights such as access to information, data protection, privacy safeguards, and the curbing of hate speech.[249] Together, these elements form the bedrock upon which a vibrant and inclusive digital civic space can flourish.

243 European Civic Forum (n 239).
244 As above.
245 As above.
246 Clarus Communications *Media trends 7 Trends in Media and How They Affect Your Success in Public Relations*. http://www.teamclarus.com/wp-content/uploads/2012/02/Media-Trends-2012.pdf (accessed 01 January 2024).
247 P Dahlgren 'The Internet as a Civic Space' in S Coleman & D Froelon (eds.) *Handbook of Digital Politics* (2015).
248 C Fernandez 'Digital rights for civil society and civil society for digital rights: how surveillance technologies shrink civic spaces' *European Digital Rights* 28 June 2023. https://edri.org/our-work/digital-rights-are-a-civic-space-issue/ (accessed 12 February 2024).
249 Roberts (n 237).

Civic freedoms necessary for an open and vibrant civic space are guaranteed by international, regional, and local instruments. This is illustrated by, among others, the UDHR,[250] ICCPR,[251] the African Charter,[252] and the Constitution.[253] Notably, the African Platform on Access to Information, 2011 asserts the obligation for governments to 'ensure that the legal frameworks create an enabling environment allowing individuals, civil society organisations including trade unions, media organisations … to fully enjoy access to information.'[254] It holds that public and private bodies have a duty to collect information for their activities, and to disperse it to citizens.[255] It further states that access to information is a fundamental right open to everyone, '[i]t is not required that anyone must demonstrate a specific legal or personal interest in the information requested or sought or otherwise required to justify seeking access to the information.'[256] Access to information may only be limited to exceptions that are strictly defined by law. The exception should be permitted if the law specifies that significant harm will be occasioned by the disclosure of the information, and the public interest in withholding the information is greater than the public interest in obtaining the information.[257] Additionally, the African Platform on Access to Information advocates for the protection of whistleblowers, stipulating that states should shield individuals from legal repercussions for disclosing information on wrongdoing.[258]

Human rights, whether exercised offline or online, warrant the same protection.[259] Every person has the right to seek and impart information on the internet in the exercise of their rights to freedom of expression and access to information. Any legal limitations on access to information are a violation of freedom of expression except in cases where such limitations are aimed at safeguarding reputations, public safety, public health, or public morals, and are deemed necessary and proportionate.[260] Furthermore, it is incumbent upon states to regulate the internet in a manner that facilitates the comprehensive realisation and amplification of human rights.[261]

The Computer Crime and Cyber Security Bill falls short in promoting an inclusive and dynamic online civic sphere due to its disregard for civic freedoms. Notably, Section 21(1) criminalises unauthorised access to computer systems, establishing severe penalties for individuals who engage in such activities without lawful justification. This approach contradicts established international norms that advocate for the unhindered enjoyment of the right to access information online. Additionally, it directly contravenes Principle 1 of the African Platform on Access to Information, which emphasises that individuals should not be required to provide a legal interest or justification for the information they seek. Consequently, the Bill unjustly curtails the fundamental right to access information. Furthermore, by failing to acknowledge the role of increased digital access as a catalyst for promoting an open and vibrant civic space, this section of the Bill overlooks a crucial aspect of digital empowerment.

250 Articles 19-20 & 2 UDHR.
251 Articles 19, 21, 22 & 25 ICCPR.
252 Articles 9-11, 13 & 2 African Charter.
253 Sections 14-16, 20 Constitution.
254 APAI (n 44) 4.
255 Key principle 13 African Platform on Access to Information.
256 Key principle 1 African Platform on Access to Information.
257 Key principle 8 African Platform on Access to Information.
258 Key principle 11 African Platform on Access to Information.
259 See Principles 5-6 & 37 ACHPR 2019 Declaration.
260 Principle 3 & 4 African Declaration on Internet Rights and Freedoms.
261 Principle 12 African Declaration on Internet Rights and Freedoms.

The Bill introduces a significant obstacle with regard to offences related to data espionage and inducement to deliver electronic messages. According to its provisions, individuals who intentionally acquire computer data for themselves or others without lawful justification or excuse, when said data is not intended for them, are deemed guilty of data espionage.[262] The Bill further states that a person who induces another, who is in control of an electronic device, to share data that is not meant for them is guilty of an offence of inducement to deliver e-messages. [263] By imposing such restrictions, this section constrains the public from freely accessing and exchanging information. Consequently, it undermines the fundamental rights of individuals to access and disseminate information, as well as their rights to freedom of expression and association.

Section 24 (2) (a) of the Bill presents another challenge. It declares that any individual who intentionally, without lawful justification, transmits, communicates, or divulges computer data to an unauthorised recipient commits the offence of illegal data interference. Subsection (c) further penalises individuals for accepting computer data without authorisation, carrying the threat of fines or imprisonment. Besides the Bill's unwarranted requirement for justification in information communication, this provision also encroaches on the public's rights to share and receive information. Such limitations undermine the principles of unrestricted access to and the free flow of information, as well as impinging on freedom of expression. Consequently, the Bill may instil apprehension among citizens and civil society organisations, discouraging them from securing, sharing, or receiving information without explicit justification, for fear of prosecution. This could lead to self-censorship among the public, diminishing social media activism, while civil societies may find it challenging to fulfil their democratic functions. Withheld information obstructs the public's ability to engage in governance, thus constituting a constraint on the right to participate fully.

Furthermore, the Bill's definition of the offence of 'cyber terrorism' poses significant concerns. It defines cyber terrorism as the deliberate, and unjustified, utilisation of a computer 'to communicate information intended to seriously intimidate a population, destabilise or destroy the fundamental political, constitutional, economic, or social structures of a country or an international organisation'.[264] This provision imposes constraints on individuals and civil societies, undermining their ability to engage in civic education, demand accountability from governmental agencies, and mobilise to exert influence on political and social structures. Consequently, it jeopardises the openness of civil discourse and undermines the principles of democratic governance.

Additionally, the Bill's definition of the offence of misuse of devices violates civic freedoms. The offence includes the act of producing, using, selling, importing, exporting or distributing a computer password or similar data that renders a computer system accessible, without justification or lawful excuse.[265] It also limits the right of access to information and fails to recognise an essential element of a vibrant civic space: the expansion of digital access through increased internet access.

Section 38 of the Bill which defines the offence of unsolicited messages, exhibits a certain disregard for civic freedoms. It renders the act of using a computer system to share multiple messages, without justification, with the intention to mislead or deceive, or the use of a device

262 Section 26 Computer Crime Bill.
263 Section 48 Computer Crime Bill.
264 Section 27 Computer Crime Bill.
265 Section 29 (1) (a) (ii) Computer Crime Bill.

that does not reveal the origin of a message, or falsifies a header of a message, an offence.[266] While the aforementioned analysis reinforces the conflict between the Bill's mandate for justification in accessing or disseminating information and the right to information access, this section compounds the issue with its utilisation of vague and expansive language, such as labelling messages as 'deceptive' or 'misleading'. The absence of clear criteria to determine the degree of deception or misleading nature of messages curtails freedoms of expression, thought, and association.

Moreover, Section 38 infringes upon the fundamental right to online privacy. By criminalising online communication without disclosing one's location, the Bill essentially compels individuals to divulge the origins of their messages. Yet, as highlighted earlier, states should uphold citizens' rights to utilise digital privacy-enhancing tools like VPNs, pseudonymous accounts, or similar technologies to safeguard their identities and ensure secure online interactions.[267] Failure to do so will leave traces of their location, thus enabling unauthorised digital surveillance by the government, contrary to right to privacy, and facilitating their possible arrests for online speech.[268]

The African Platform on Access to Information stipulates that states are obligated to safeguard whistleblowers who face legal repercussions for disclosing information about misconduct. However, the clauses outlined in the Bill diverge from these international norms, as they impose penalties on whistleblowers, running counter to established standards.

While the Bill is lauded for establishing the National Cyber Security Advisory Council (NCSAC), it falls short by excluding representation from civil societies, human rights activists, and the media from its membership.[269] This oversight neglects crucial stakeholders in the civic space. The functions of the Council are, among others, to advise the government on matters of cyber security such as policy development and cyber security strategies, and to identify and adopt cyber security best practices. Cyber security refers to the protection of the confidentiality, integrity and availability of information in the cyber environment and the protection of internet users' assets. As such, it includes preserving privacy rights, ensuring data protection, and upholding the rights of access to and free flow of information.

As previously highlighted, states should permit civil societies and individuals to actively engage in public discourse and contribute meaningfully to the development of policies. This engagement serves as a vital mechanism for addressing challenges to the rule of law, democracy and fundamental rights and freedoms. The African Declaration on Internet Rights and Freedoms mandates civil societies to 'advocate for internet rights and freedoms; monitor internet laws and regulations; and highlight abuses.'[270] Similarly , the UN recognises the significance of civic space in its Sustainable Development Goals (SDGs) 16 and 17. SDG 17 encourages effective partnerships between the public (government) sector, private sector and civil societies for development.[271] SDG 16 encourages states to '[e]nsure responsive, inclusive,

266 Section 38 (1) (a) & (b) Computer Crime Bill.
267 L Nitsche 'Digital Rights: Civic space continues to be constrained' *Akademie* 04 May 2018. https://p.dw.com/p/2x2tf (accessed 18 February 2024).
268 For a discussion of the offence of Publication of false information see Section 43 of the Computer Crime Bill, Sec 4.1 on Cybersecurity and Sec 5.5 Misinformation and Disinformation above.
269 Section 3 (1) & (4) Computer Crime Bill.
270 African Internet Rights (n 44) 29.
271 The Global Goals '17 Partnerships for the goals' https://www.globalgoals.org/goals/17-partnerships-for-the-goals/ (accessed 15 January 2024).

participatory and representative decision-making at all levels.'[272] By excluding representation from the civic space in the National Cybersecurity Advisory Committee, the Bill runs counter to established international norms of development and democracy, thus further narrowing the digital landscape for civic participation.

None of the Bills' limitations on civic freedoms is justified. It neither indicates the harm that will be suffered if the rights are not limited nor does it show that the rights preserved are superior to the rights it limits. The limitations also do not fall within the permitted scope of the ACHPR 2019 Declaration, the African Declaration on Internet Rights and Freedoms or the Constitution.[273]

In summary, the above provisions of the Computer Crime and Cyber Security Bill render an open and vibrant digital civic space unsustainable. It falls short in safeguarding this space, posing a threat to civic freedoms by sanctioning arrests for online expression and endorsing digital surveillance, thereby undermining civil participation in a democratic society. A vibrant and secure civic space is necessary for the protection and development of media and digital rights and freedoms.[274] Unjustifiable and unreasonable restrictions on the operations of the civic space undermines human rights.

Notably, while the public now has diverse avenues of engagement in the online civic space, this trend has contributed to the shrinking of traditional media. The decline of newspapers and magazines is evident as readers increasingly rely on the internet for news consumption.[275] Online reporters are on the rise.[276] Concurrently, the emergence of online reporters, particularly bloggers, has increased. Unlike traditional journalists, bloggers often lack formal journalistic training or background, yet wield significant influence in reporting.[277] This phenomenon poses a challenge to the stability and sustainability of conventional media structures. Due to a lack of professional training, bloggers frequently disregard journalistic protocols, foregoing fact-checking and source verification before disseminating information. They tend to disclose their sources and sometimes hack resources. Since they are not journalists, they do not have to conform to non-biased publications. Consequently, there is a risk of spreading misinformation.[278] Nonetheless, the regulation of misinformation is covered by part 5.6 of the report below.

Recommendations

The following recommendations are proposed to the Ministry of Communications, Science and Technology to enhance media and civic space sustainability in the digital age. The Computer Crime and Cyber Security Bill should be amended as follows:

- Amend section 21 on the offence of illegal access, by removing the requirement for a lawful excuse for access to a computer system and access to computer data, and phrase

272 The Global Goals '16 Peace, Justice and Strong Institutions'. https://www.globalgoals.org/goals/16-peace-justice-and-strong-institutions/ (accessed 20 February 2024).
273 The instruments permit limitations of rights if the limitations are for protection of one's reputation, public safety, public health or public morals.
274 OECD 'Civic Space' https://www.oecd.org/fr/gov/gouvernement-ouvert/civic-space.htm (accessed 08 February 2024).
275 Clarus Communications (n 246).
276 Advertisement revenues are also down due to the reduced number of readers offline, leading to shutdown of newspaper houses and newspapers establishing an online presence.
277 Clarus Communications (n 246).
278 As above.

the offence as suggested in recommendation (a) of part 4.2 above. Alternatively, to eliminate the offence of illegal access from the Bill.
- Amend section 26 on the definition of data espionage by deleting "without lawful excuse or justification or in excess of lawful excuse or justification" and "which are not meant for him", to ensure clarity and coherence in the legal framework.
- Delete the offence of inducement to deliver electronic messages in section 48.
- Delete section 24 (2) (a) & (c) on illegal data interference.
- Amend the definition of cyber terrorism in section 27 to exclude the words 'seriously intimidate a population, destabilise or destroy the fundamental political, constitutional, economic, or social structures of a country or an international organisation'. Instead, broaden the description to include the use of computer data that poses threats of death, intimidation, or kidnapping.
- Amend the offence of misuse of devices by deleting section 29(1)(a)(ii).
- Delete the offence of unsolicited messages in section 38. The existing provisions in Section 36 of the Electronic Transactions and Communications Bill 2022 sufficiently address concerns related to unsolicited messages.
- Expand the composition of the NCSAC, under section 3(4) and include representatives of civil societies, media, and human rights activists. This will ensure a more inclusive and diverse representation in cybersecurity policy making processes.
- Collaborate between the Ministry and civil society organisations to enhance knowledge and capacity-building initiatives for the public on the use of digital security tools such as VPNs. This proactive approach will empower individuals to protect their digital privacy and security effectively.

These proposed amendments are designed to promote a balanced legal framework that addresses contemporary challenges in cybersecurity while safeguarding individual rights and promoting digital innovation.

5.3 Media diversity in the digital age

Media diversity is a cornerstone of freedom of expression, facilitating a rich tapestry of voices representing diverse perspectives within society. It serves as a platform for various groups to articulate their opinions and advocate for their interests, thereby enriching public discourse. Moreover, a diverse media landscape ensures that society has access to a wide range of information, empowering individuals to engage meaningfully in democratic processes. Principle 11(3) of the ACHPR 2019 Declaration articulates the importance of media diversity by promoting pluralistic media, non-discriminatory and non-stereotyped information, ensuring transparency and diversity in media ownership, and promoting the use of local languages in public affairs.

The proliferation of digital media in Lesotho Is contributing to media diversity in the online space. As of May 2024, Lesotho had two electronic media houses alongside a plethora of online platforms such as blogs, online newspapers, and internet-based television and radio stations.[279] This expanding digital landscape offers an unprecedented opportunity for a wide range of voices and perspectives to be heard, enriching the media landscape and promoting greater inclusivity in public discourse.

279 Press Reference 'Lesotho Press, Media, TV, Radio, Newspapers forum' http://www.pressreference.com/Ky-Ma/Lesotho.html; MISA Lesotho 'Media Directory'. https://lesotho.misa.org/media-directory/ (accessed 09 May 2024). Lesotho also has 27 radio stations,11 newspapers, 3 magazines and 1 national television station. Two of the radio stations formerly broadcast in English and Sesotho languages.

In 2021, the Parliament adopted a National Media policy, with one of its primary objectives being the promotion of a vibrant and diverse private media landscape. Due increased internet accessibility and the active implementation of this policy, the Basotho can showcase their independent print publications, videos, and music, while also enjoying enhanced access to a wealth of web-based content.[280] The internet serves as a dynamic platform for promoting discussions on political satire, as well as issues concerning and Lesbians, Gays, Bisexual, Transgender, Queer, Intersex, and Asexual (the LGBTQIA community) and other pertinent socioeconomic and political conversations.[281] However, despite these strides, there is a notable tendency within Lesotho media to focus more on political leadership at the expense of other vital areas such as justice issues and community news.[282] Nevertheless, Lesotho is steadily progressing towards the realisation of digital rights through the promotion of media diversity, a journey marked by ongoing efforts to broaden the scope of information dissemination and ensure a more inclusive representation of societal voices and concerns.

5.4 Hate speech, harassment, and incitement to violence

Freedom of expression is a cornerstone of democratic societies, yet it should be balanced with the necessity to prevent harm. Hate speech, harassment, and incitement to violence are clear instances where the boundaries of free speech should be drawn. Some international instruments such as the ICCPR expressly prohibit these actions. Article 20 provides that '[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.'[283] Similarly, the ACHPR 2019 Declaration, which extends the basic human right to the internet, has similar stipulations.[284] It provides that states should criminalise hate speech 'as a last resort and only for the most severe cases.'[285] To determine the severity of a case, states must consider, among other factors, the prevailing social and political situation, the speaker's influence, and the intent to incite harm. Moreover, Article 4 of the UN International Convention on the Elimination of All Forms of Racial Discrimination[286] mandates states to combat racial hatred and propaganda, while the UN Resolution on interreligious and intercultural dialogue condemns the spread of hatred through social and electronic media.[287] These measures collectively uphold the principle of free expression while safeguarding against its abuse to propagate bigotry and violence.

Although not specific to hate speech, harassment or incitement, the Constitution permits the limitation of freedom of expression in the interests of public safety and public order, or for the protection of the reputation of others.[288] In 2017, the government temporarily shut down MoAfrica FM, for 72 hours amid accusations of inciting violence and using hate speech.[289] The radio station had facilitated the registration of victims of police brutality by a self-exiled former

280 UNESCO 'Lesotho Media policy draft 2009' (2009). https://en.unesco.org/creativity/policy-monitoring-platform/lesotho-media-policy-draft-2009 (accessed 24 May 2023).
281 MISA Zimbabwe (n 195) 9.
282 MISA Zimbabwe (n 195) 43.
283 Article 20 (2) ICCPR.
284 Principle 23(1) of the ACHPR 2019 Declaration.
285 Principle 23 (2) (c) of the ACHPR 2019 Declaration.
286 United Nations General Assembly 'Resolution 2106 (XX): International Convention on the Elimination of All Forms of Racial Discrimination' (1965) https://www.ohchr.org/sites/default/files/cerd.pdf (accessed 24 May 2023).
287 United Nations General Assembly 'Resolution A/RES/73/328: Resolution on Promoting interreligious and intercultural dialogue and tolerance in countering hate speech' (2019) para 2 https://digitallibrary.un.org/record/3814328?ln=en (accessed 12 August 2023).
288 Section 14 (2) of the Constitution.
289 The Post (n 1).

deputy leader of the Lesotho Congress Party, for interviews with Amnesty International. It also criticised the then Prime Minister's encouragement of police brutality. Section 14(4) of the Constitution permits individuals offended by statements on a communication platform to respond or correct them on the same platform. However, the aggrieved party did not utilise this opportunity, the speaker lacked significant influence over the radio's audience, and there was no evident intention to incite violence. Consequently, the government's decision to shut down the radio station raises doubts about its conformity to constitutional and international norms.

As already indicated, the legal framework of Lesotho, particularly articulated in the Penal Code Act, imposes restrictions on the exercise of freedom of expression in instances where such limitations are deemed necessary. The Act proscribes the dissemination of information or the expression of sentiments that harbour hatred or disdain toward identifiable groups based on characteristics such as race, gender, disability, or ethnic origin.[290]

The Computer Crime and Cyber Security Bill safeguards against certain prohibited acts in the digital space. Specifically, the Bill criminalises the intentional and unlawful production, offer, distribution or transmission of information or language, through computer systems, which incites or aids acts of discrimination, notably those targeting individuals or communities on the grounds of race, gender, disability, or ethnicity. This includes materials that promote or assist in perpetrating racist, homophobic, or xenophobic acts,[291] as well as those that instigate or solicit others to engage in genocide or crimes against humanity.[292] The Bill also extends its reach to address the pervasive issues of cyberbullying and harassment, recognising these behaviours as actionable offences deserving legal redress.[293]

Although Lesotho's legal apparatus stands as a safeguard against the propagation of hate speech, both in the digital sphere and traditional mediums, it is essential to acknowledge that the application of these legal provisions has not been devoid of criticism. Instances have arisen wherein state authorities have been accused of overreach, evidenced by cases such as the unjustifiable closure of certain media outlets, including radio stations, which has raised concerns regarding the potential abuse of limitations on freedom of expression.

5.5 Defamation

Defamation constitutes 'writ[ing] or say[ing] something that damages someone's reputation.'[294] It can either be a civil wrong or a criminal offence. Criminal defamation occurs when a state charges a person with defamation, and they are punished by payment of a fine or imprisonment.[295] Under common law, an aggrieved party can pursue civil remedies against the perpetrator. In such cases, the aggrieved party may seek damages as compensation for harm caused to their reputation. This legal framework surrounding defamation serves as a mechanism to balance the right to freedom of expression with the need to safeguard individuals' reputations from unwarranted harm.[296]

290 Section 79 Penal Code Act.
291 Section 35 & 36 Computer Crime and Cyber Security Bill.
292 Section 37 Computer Crime and Cyber Security Bill.
293 Section 40 Computer Crime and Cyber Security Bill.
294 Oxford *South African Pocket Dictionary* (2015) 229.
295 Limpitlaw (n 193) 337.
296 SALC Litigation Manual Series 'Freedom of Expression: Litigating Cases of Limitations to the Exercise of Freedom of Speech and Opinion' (2016) 27. https://www.southernafricalitigationcentre.org/wp-content/uploads/2017/08/Chapter-4.pdf (accessed 18 May 2023).

The ACHPR 2019 Declaration outlines fundamental standards concerning defamation laws, aiming to safeguard the right to freedom of expression. These standards are articulated in three provisions: 'a. no one shall be found liable for true statements, expressions of opinion or statements which are reasonable to make in the circumstances. b. public figures shall be required to tolerate a greater degree of criticism. c. sanctions should never be so severe as to inhibit the right to freedom of expression.'[297] These principles provide guidance in regulating the scope of freedom of expression, particularly concerning online discourse.

The ACHPR Resolution on repealing criminal defamation called on states to refrain from imposing rules that violate freedom of expression; to repeal criminal defamation laws that impede freedom of speech; and to adhere to principles of freedom of expression enshrined in both the African Charter and ICCPR. It highlights the importance of upholding journalistic ethics and standards. It encourages 'journalists and other media practitioners to respect journalism ethics and standards in gathering, reporting, and interpreting accurate information, so as to avoid restriction to freedom of expression, and to guide against risk of prosecution.'[298] By doing so, they mitigate the risk of legal prosecution and safeguard the exercise of freedom of expression.

Lesotho has adhered to the Resolution on repealing criminal defamation by setting aside section 104 of the Penal Code, a move reinforced b The High Court sitting as the Constitutional Court in *Basildon Peta v The Minister of Law and Constitutional Affairs and Human Rights and Others* CC/11/2016 held that the Penal Code section was inconsistent with section 14 of the Constitution which provides for freedom of expression.[299] This is especially so when there are civil remedies available for defamation. The court held that criminal defamation makes media persons apprehensive of reporting to the public, thus violating freedom of expression.

In 2017, the government shut down two radio stations, namely Tšenolo FM and People's Choice FM, on allegations of broadcasting defamatory material of political leaders.[300] The shutdown actions negatively affect freedom of expression and the right of access to information. Therefore, they should be avoided.

However, the Computer Crime and Cyber Security Bill reintroduces the concept of criminal defamation by criminalising the publication of false information.[301] This is because the offence of publication of false information has a similar effect to criminal defamation. Criminal defamation is the act of publishing untrue information that may injure the reputation of another person with an intent to defame that other, which act, attracts criminal punishment. The Bill therefore does not conform with international standards on protection of freedom of expression to this extent.

---

297 Principle 21 of the Declaration on Freedom of Expression.

298 The ACHPR further expressed concern at the deteriorating press freedom in some parts of Africa, and in particular: restrictive legislations that censor the public's right to access information; direct attacks on journalists; their arrest and detention; physical assault and killings, due to statements or materials published against government officials.

299 *Basildon Peta v Minister of Law, Constitutional Affairs and Human Rights and Others*, Case No. CC 11/2016 https://media.lesotholii.org/files/judgments/lshc/2018/3/2018-lshc-3.pdf (accessed 14 May 2023).

300 'Government closes two Lesotho radio stations over criticism' *Misa Lesotho* 10 February 2017 (accessed 13 May 2023).

301 Section 43 Computer Crime and Cyber Security Bill. Tšosane quoted in The Reporter 'Cyber law slammed, again' *The Reporter* 15 December 2023 https://www.thereporter.co.ls/2022/12/15/cyber-law-slammed-again/ (accessed 13 May 2023).

5.6 Disinformation and misinformation

Misinformation and disinformation spread rapidly to masses of people due to speedy communication through social media and other digital platforms, often leading to violations of human rights.[302] The problem is compounded by the monetary reward that internet users receive from social media houses when they post more content online and gain large numbers of followers.[303] While there is no specific definition of these concepts, disinformation can be defined as false information that is deliberately created and spread to mislead or deceive.[304] On the other hand, misinformation is the act of giving wrong informationabout something.[305] This report will refer to both misinformation and disinformation and false news interchangeably. False news includes conspiracy theories about health policies and vaccines, smear campaigns that undermine certain groups in society, and false news about state officials and political parties.[306]

Misinformation and disinformation lead to violations of several human rights. For one, the overflooding of untrue information influences and changes people's minds. They are unable to formulate opinions based on facts, and their freedom to formulate their own beliefs is undermined. Thus, their freedom of thought, which is guaranteed by Article 18 of the ICCPR is compromised.[307] False news also compromises the right to health guaranteed by Article 12 of the ICESCR. Conspiracy theories about health policies that address certain diseases, and the effects of vaccines, may influence the recipients of the information to refuse treatment to protect their health and that of others. This negatively affects the right to health.

Further, misinformation and disinformation affect the right to free and fair elections provided by Article 25 of the ICCPR. False news about political parties, their campaigns and candidates give the public wrong impressions about the candidates and may induce and manipulate the electorate to vote differently from what they would have if they had accurate information. This tampers with the right to vote freely and fairly. Smear campaigns that undermine minority groups of society such as ethnic groups, compromise the right to non-discrimination provided by the ICCPR.[308] The smear campaigns can incite hostility, violence, attacks and or killings of the persons in the targeted groups. The people's right to life and the right to freedom and security are violated.[309] Yet, under international human rights standards, these rights are available to all persons without distinction.

Interestingly, state responses to misinformation and disinformation online have also posed challenges to digital rights. States develop policies and regulations that are meant to control false news by either criminalising the acts or restricting certain publications. However, the measures tend to disproportionately intimidate critical voices and limit the right to freedom of opinion and to access and share information of the media and human rights activists. The

302 'Digital disinformation and human rights explained' *Global Partners Digital* 01 June 2023 https://www.gp-digital.org/a-human-rights-based-approach-to-disinformation/ (accessed 05 June 2023).
303 Amnesty International (n 307).
304 Oxford (n 294) 254
305 Oxford *Advanced Learners dictionary* (2005) 939.
306 'Freedom of expression is key to countering disinformation' United Nations Human Rights Office of the High Commissioner 03 November 2022 https://www.ohchr.org/en/stories/2022/11/freedom-expression-key-countering-disinformation (accessed 05 August 2023).
307 Amnesty International 'A human rights approach to tackle disinformation submission to the office of the high commissioner for human rights' (2022) https://www.amnesty.org/en/wp-content/uploads/2022/04/IOR4054862022ENGLISH.pdf (accessed 06 August 2023).
308 Article 6 (1) & 26 ICCPR.
309 Articles 6 & 9 ICCPR.

restrictions consequently inhibit their rights to freedom of expression and the free flow of information online. It follows that states should develop human rights-based approaches that respect freedom of expression so that online media is not constricted by fear but continues to flourish and the public is not denied their right to information.

Lesotho has developed legal instruments that attempt to curb the publication of misinformation and disinformation to protect digital rights at risk.[310] For example, in Section 3(f) of the Declaration of COVID-19 State of Emergency Notice and Section 10(1) of the Public Health (COVID-19) Regulations 2020, it is an offence to publish false news.

The Computer Crime and Cyber Security Bill also regulates disinformation and misinformation in cyberspace. It makes the publication of false information that is deceptive, inaccurate, or misleading, intending to mislead or deceive the public an offence.[311] Despite the challenge that the offence effectively resuscitates criminal defamation, it does not clarify who is responsible for determining that information is misleading. Nonetheless, the risk of identifying such a party is that the state will place powers of interpretation of people's expression, in the hands of another. This will effectively violate the right to freedom of opinion and expression.

Another problem with the Computer Crime and Cyber Security Bill is that the Bill does not define the terms 'false information', 'mislead' or 'deceive' under its criminalisation of publication of false information. The Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda 2017, states that vague and ambiguous statements such as 'false news' are not compatible with human rights.[312] This is because human rights do not permit general restrictions to the interpretation of events or erroneous opinions.

The COVID Regulation and Notice, together with Bill, instil fear into the press and other internet users to inform the public. They self-censor, lest they are criminally charged with distributing false information that is deceptive or misleading. The regulations constrain the media and internet user's freedom to express their opinions.

The Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda 2017 states that freedom of expression should not be restricted unless the restriction is justified. That is, the restriction should be by a legal instrument, for a legitimate interest that is recognised by international law, and is necessary and proportionate to protect the interest.[313] The Lesotho Regulation and Bill do not meet the criteria as they are not necessary nor proportionate to protect freedom of expression. They are thus incompatible with human rights standards.

Section 7(1) of the Broadcasting Code provides a neutral approach. It states that news should be reported accurately and fairly, without any negligent or intentional distortion, exaggeration, or material omission of facts. Instead, a broadcaster should present as facts, only reasonably true matters. The Code is non-restrictive but encourages the publication of accurate news. It is consistent with human rights standards.

310 Lesotho Communications Authority 'Warning on distribution of false and fake information using communications platforms' https://lca.org.ls/warning-on-distribution-of-false-and-fake-information-using-communications-platforms/ (accessed 17 May 2023).

311 Section 43 Computer Crime Bill.

312 Organisation for Security and Co-operation in Europe 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda' (2017) para 2(a) https://www.osce.org/fom/302796 (accessed 15 September 2023).

313 As above.

Apart from regulations, the Internet Society Lesotho Chapter, a global cause-driven organisation with a mandate to promote local and regional views on emerging internet issues,[314] held a training on false news, misinformation, and disinformation in 2020. The objectives of the training were to raise awareness about the problem of false news among internet users in Lesotho, the legal implications of false news, how to tackle false news, and the skills required to verify internet information.[315] This is a significant effort in curbing false news while promoting freedom of expression online.

Recommendations

- The Ministry of Communications, Science and Technology to expunge Section 43 that criminalises false information from the Computer Crime and Cyber Security Bill.
- The Ministry of Health should amend the Declaration of COVID-19 State of Emergency Notice and the Public Health (COVID-19) Regulations 2020 to remove the criminalisation of publishing false news.
- State authorities, such as government ministries, should build reliable and swift news outlets which publish accurate, evidence-based, trustworthy information which is accessible to the public. The information will counter false and misleading information and deter publications of false or misleading information. These mechanisms will increase public trust in the reliability of the information.[316] At the same time, preserving the rights of the media and internet users to communicate their opinions freely, and preserving the other human rights that are negatively affected by the misinformation. This action will be in line with the Model Law on Access to Information for Africa. The Model Law requires public bodies to publish information such as policies, manuals, procedures and rules made by the bodies which affect the public; and provide the names, addresses and email addresses of the responsible officers and their designations, where the public may submit their requests for the information.[317]
- Lesotho should create an environment that enables freedom of expression. It should 'promote a free, independent and diverse communications environment, including media diversity' to counter misinformation and disinformation.[318] This includes numerous information sources to allow different opinions. Additionally, enabling media that can, without fear, invite public officials and state actors to explain or defend their positions, engage in public debates and respond to misinformation to allow the public to be informed with accurate information.[319]
- State actors should refrain from sponsoring or encouraging publications which do not verify facts before posting them or disseminating propaganda.[320]
- Lesotho should promote education on digital literacy and media. The objective is to capacitate the public with knowledge to distinguish between verified and unverified information and to establish accurate information. This may be achieved by the Ministry of Education including subjects on the matter in education curriculums, and civil societies raising awareness on the issue.[321]

314 Internet Society Lesotho Chapter 'About Us' https://isoc.org.ls/about-us/ (accessed 07 May 2023).
315 'Fake news, Misinformation and Disinformation' *ISOC Lesotho* 16 November 2020. https://isoc.org.ls/news/fake-news-misinformation-and-disinformation/ (accessed 06 August 2023).
316 Amnesty International (n 307) 13.
317 Article 7 ACHPR Model.
318 OSCE *et al* (n 312) para 3a.
319 Amnesty International (n 316).
320 OESC *et al* (n 312).
321 Amnesty International (n 319).

- Although it might be tempting for the state to authorise some companies to define the terms 'false information', 'deceptive', 'misleading' and other vague words, it should desist from doing so because it will be handing over public rights to form their opinions to the companies.
- The Ministry of Communications, Science and Technology should develop a policy on how to curb the spread of misinformation and disinformation on social media platforms.

5.7 Online content governance

Content governance is a process that involves reviewing and moderating content that users place online to ensure that it complies with certain policies and guidelines.[322] It involves the removal of content from an online space which may be considered offensive or illegal,[323] or downgrading the visibility of content.[324]

Content governance negatively affects the right of access to information and freedom of expression[325] online which laws have guaranteed and states need to facilitate.[326] The African Declaration on Internet Rights and Freedoms stipulates that content blocking, removal or other legal restrictions on access to content on the internet is a grave infringement of freedom of expression online.[327] Principle 39 of the ACHPR 2019 Declaration provides that states should require internet intermediaries to enable access to information on the internet without discrimination of the content. They should not block or prefer certain internet traffic information over others. It sets out conditions under which internet intermediaries may remove content online. Among these, is that the request for removal of content should be valid and consistent with human rights laws and standards.[328] That is, it is permissible only if it protects a legitimate interest, and is necessary and proportionate to the protected interest.

The ACHPR 2019 Declaration further advocates for media independence. It stipulates that media owners and practitioners should develop policies that guarantee their editorial independence and freedom from commercial or political influence over their content.[329] Lesotho should promote a free, pluralistic, and independent media for the maintenance of a democratic nation, in recognition of the Constitution and international human rights standards.

The LCA has proposed the promulgation of Internet Broadcasting Rules, 2020, which are meant to regulate online radio stations, internet broadcasting and content distributed over the internet.[330] The Regulations define an internet broadcaster as any internet user with a minimum of one hundred (100) followers. It also defines an internet broadcast as a post on social media that reaches 100 people.[331] A post is any video, audio, picture or message that is uploaded on

322 Besedo 'What is content moderation?' https://besedo.com/knowledge-hub/blog/what-is-content-moderation/ (accessed 17 May 2023).
323 As above.
324 Centre for Human Rights (n 2) 38.
325 As above.
326 Principle 37 (1) of the ACHPR 2019 Declaration.
327 Pan-Africa. *The African Declaration on Internet Rights and Freedoms*. https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf [Accessed: 2023.08.03].
328 Principle 39 (4) (d) of the ACHPR 2019 Declaration.
329 Principle 12 (3) of the ACHPR 2019 Declaration.
330 'Lesotho proposed internet broadcasting rules will stifle free speech' *MISA Zimbabwe* 6 October 2020. https://zimbabwe.misa.org/2020/10/06/lesotho-proposed-internet-broadcasting-rules-will-stifle-free-speech/ (accessed 16 May 2023).
331 As above.

the internet. The Rules require all broadcasters to register with the LCA, to comply with the Broadcasting Rules of 2004 (currently repealed by Broadcasting Code 2022). The Regulations permit the Authority to remove content posted on the internet.[332]

It is noted that the Rules' use of the word 'followers' is vague, it can therefore imply that it regulates Facebook and Twitter largely used in Lesotho. The Rules imply that they will also cover individuals who communicate through X (formerly Twitter), Facebook, YouTube, TikTok, Google and other internet platforms. If the Rules are promulgated as they are, and content removal clauses are enforced on the broadcaster and broadcasts, it will have an effect of restricting the broader population's freedoms of expression and opinion online, and media freedom, contrary to international standards. The instrument is, therefore, to be closely monitored to ensure that it is consistent with international human rights and does not diminish media independence.

The Computer Crime and Cyber Security Bill provides for content moderation as well. It states that a Hosting provider or a Hyperlink provider, will not be liable for illegal information posted where they disable or remove the information expeditiously upon receipt of a court order to do so, or if they have learnt about the illegal information by other means.[333] The Bill protects freedom of expression online to this extent.

The Internet Society Lesotho Chapter, in collaboration with the Ministry of Communications, Science and Technology, hosted a School of Internet Governance in Lesotho, and an Internet Governance Forum in Maseru in 2020. The objective of the school was to capacitate internet stakeholders and policymakers on internet governance. This was meant to help improve the decisions of policymakers when regulating and governing the internet, leading to increased socio-economic development in the country. The training was also meant for the participants to share their knowledge with internet users in their respective communities, to ensure a safe and free internet.[334]

Recommendations

- The Ministry of Communications, Science, and Technology should revisit the Internet Broadcasting Rules of 2020, specifically focusing on refining the definitions of "followers" and "posts" to ensure clarity and relevance in the digital context.
- Additionally, the Ministry should consider eliminating the provision related to content removal within the Internet Broadcasting Rules, 2020, as it may impede freedom of expression and access to information online.
- Furthermore, to enhance capacity and expertise in internet governance and online content regulation, the Ministry of Communications, Science, and Technology should proactively support and finance a broader array of training initiatives in this domain.

332 MISA Zimbabwe (n 195) 20.
333 Section 69 & 71 of Computer Crime Bill.
334 M Letuka 'First School of Internet Governance' *Public Eye* 16 August 2021 https://publiceyenews.com/first-school-of-internet-governance-hosted/ (accessed 7 August 2023).

CHAPTER 6
SURVEILLANCE

6. SURVEILLANCE

On the one hand, surveillance is the act of watching a person or place, by the police, because a crime has occurred or it is anticipated that it will occur.[335] Government surveillance, on the other hand, refers to the act of collecting information on a person or group of persons by an ongoing observation of their communication, place or actions to gather intelligence, conduct a lawful investigation of a crime or for social control.[336] Online surveillance is conducted by observing networks and information processing, including collecting contents of electronic communications and their metadata and watching computer systems.[337] In summary, surveillance intercepts communication between two or more parties to hear what they are planning.[338]

Surveillance infringes on the right to privacy and freedom of expression. To elaborate by example, surveillance poses a threat to whistle-blowers' privacy. Journalists require whistle-blowers to assist them with investigational journalism. If whistle-blowers are afraid to provide information because their identities will be revealed through surveillance, it means that the public's freedom of expression is curtailed, the media cannot access or impart information, and democracy is gravely threatened.[339] Thus, states should protect their rights.[340]

International human rights legal instruments guard against violation of privacy by surveillance. Principle 41(1) of the ACHPR 2019 Declaration provides that '[s]tates shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications.' Instead, they should engage in surveillance only if it is authorised by law, has a specific target and conforms with human rights laws, investigates a crime or has a legitimate objective. The law authorising the surveillance should have proper safeguards for the protection of privacy. For instance, it should require a judicial authority to authorise the surveillance, the surveillance should be for a clear duration, scope and coverage and specify the place involved, the surveillance method should be transparent on the nature of its operations, and it should be monitored by an independent oversight body.[341]

The Constitution guarantees the right to privacy and freedom of expression.[342] It permits limitations on these rights where an act is conducted under a law that serves the interests of defence, public safety, public order or public morality.[343] Lesotho further enacted the Lesotho Communications Act, Penal Code, Data Protection Act, and National Security Service Act and has a draft Computer Crime and Cyber Security Bill that deals with surveillance. The Communications Act makes it an offence for a person to intercept or trace communication operations or messages without the authority of a competent court.[344] It further makes it an offence for

335 Cambridge Dictionary 'Surveillance' https://dictionary.cambridge.org/dictionary/english/surveillance (accessed 11 August 2023).
336 Cyberwire 'government surveillance' https://thecyberwire.com/glossary/government-surveillance (accessed 05 May 2023).
337 As above.
338 WC Banks 'Cyber espionage and electronic surveillance: Beyond the media coverage' (2017) 66 *Emory Law Journal* 514. https://scholarlycommons.law.emory.edu/elj/vol66/iss3/3 (accessed 23 May 2023).
339 MISA Lesotho 'Webinar on computer crimes and cybersecurity law' https://www.youtube.com/watch?v=Qz7g1la2pmg&ab_channel=MISALesotho (accessed 29 July 2023).
340 Principle 11 African Platform on Access to Information .
341 Principle 41 (1) - (3) ACHPR Declaration of 2019.
342 Section 11 (1) & 14 Constitution.
343 Section 11 (2) & 14 (2) (a) Constitution.
344 Section 44 (1) (f) Communications Act.

a person to intentionally modify message contents through communication services.[345] This implies that the Communications Act permits surveillance but only if conducted through a court order. However, while the need for court authorisation conforms with international human rights and standards, the Act does not establish grounds for the application of an order that permits surveillance. The Penal Code makes it an offence for a person to either lawfully or unlawfully access and or interfere with a computer or electronic storage device of another, to derive information from the device or derive a benefit for themself, if they have no reason to believe that the owner would permit them to do so.[346] Therefore, the Penal Code prohibits unlawful surveillance.

However, the Computer Crime and Cyber Security Bill amends the Communications Act and Penal Code by deleting the sections on surveillance.[347] The Bill proposes to regulate surveillance under section 66. It states that a court may permit an investigation officer to install a remote or direct forensic tool onto another's computer system to collect information. A remote forensic tool is 'an investigative tool, including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks that include keystroke logging or transmission of an internet protocol address.'[348]

The court will permit the attachment of a remote forensic tool if it is part of a criminal investigation of offences stated in the Computer Crime and Cyber Security Bill, and there is proof that there are no other procedures that can be resorted to, to obtain the information.[349] The court order may direct an internet service provider to assist in the installation of the surveillance tool.

In the surveillance application, the investigation officer should show the name of the suspect and the targeted computer system, including the length of the surveillance which should not exceed three months. The information obtained through the forensic tool shall be protected from modifications or deletions. However, the Bill is silent on the timeframe within which the information may be kept and protected from modifications. Where there is a need to effect any modifications to a computer system under investigation, these should be conducted to a minimum and undone at the end of the investigation. A log of the information obtained should be kept, and a National Cyber Security Advisory Council established under the Bill must have remote access to the computer system under surveillance. The Computer Crime and Cyber Security Bill is commended for complying with principle 41 of the ACHPR 2019 Declaration.

The Computer Crime and Cyber Security Bill goes on to prescribe punishable offences. These include intentional and unlawful access to a computer system,[350] remaining logged in a computer system by defying security measures to obtain data,[351] illegal interception of computer data transmission,[352] illegal data or computer system interference,[353] and data espionage[354]. These offences can lead to unlawful surveillance.

345 Section 44 (1) (e) Communications Act.
346 Section 62 (2) of Penal Code 2010.
347 Section 79 & 80 of Computer Crime and Cyber Security Bill.
348 Section 2 of Computer Crime and Cyber Security Bill. Keystroke logging is the secret recording of the keys typed on a keyboard, done in such a way that a person using the keyboard is oblivious to the fact that they are being monitored.
349 Section 66 (1) Computer Crimes and Cyber Security Bill.
350 Section 21 Computer Crimes and Cyber Security Bill.
351 Section 22 Computer Crimes and Cyber Security Bill.
352 Section 23 Computer Crimes and Cyber Security Bill.
353 Section 24 & 25 Computer Crimes and Cyber Security Bill.
354 Section 26 Computer Crimes and Cyber Security Bill.

Although Lesotho enacted the Communications Regulations with the intent to curb cybercrime and other offences,[355] registration of personal information stored by a licensee can be easily accessed by the government and security services. This can enable the government to easily monitor the communications of a subscriber without a court order. Moreover, the Regulations mandate the collection of private data for no specific crime. Its limitation of privacy does not meet the standard that privacy may be limited where it is necessary since there is no specified crime to combat. Lastly, the Regulations do not provide an oversight mechanism over the surveillance. In other words, a data subject does not have a body to seek redress from if they have complaints about the licensee's data collection. Thus, the regulations violate data protection laws.

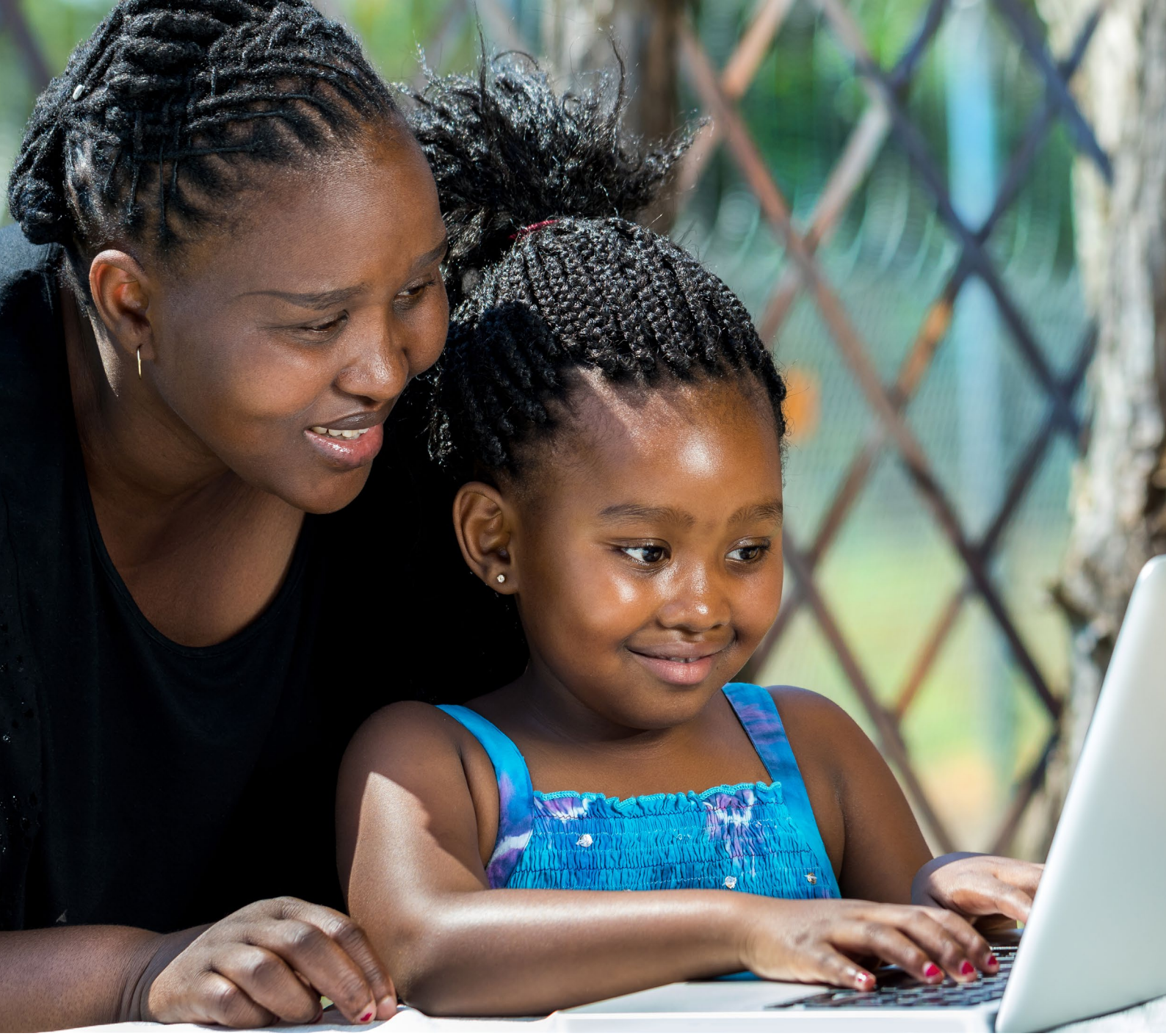
It is noted that the National Security Services Act permits a member of the National Security Service to intercept communication on a telephone or telecommunications line with the authority of a Director General or Prime Minister.[356] Although it could be challenged that the permission of surveillance without a court's authorisation violates the right to privacy, it is allowed in the interests of defence or public order, and acceptable under the Constitution. It is, however, important that some safeguards are exercised to avoid abuse of power. Thus, the Act's limitation of the rights should be justified by a legitimate aim, necessity and proportionality of interests protected.[357]

Recommendations

The following recommendations are proposed to enhance data protection measures within the Communications (Subscriber Identity Module Registration) Regulation, thereby safeguarding the privacy and rights of individuals and mitigating the risk of unlawful surveillance.

- The Ministry of Communications, Science and Technology should amend the Communications (Subscriber Identity Module Registration) Regulation to include stronger safeguards for the protection of collected data. This may involve implementing encryption protocols, stringent access controls, and regular audits to prevent unauthorised access or misuse of personal information.
- The Ministry should ensure that any amendments to the regulation align with established privacy standards and regulations. This may involve conducting thorough privacy impact assessments to identify and mitigate potential risks to data privacy.
- The Ministry should introduce provisions that promote transparency and accountability in the handling of collected data. This includes requirements for clear and accessible privacy policies, mechanisms for individuals to access and correct their personal data, and avenues for lodging complaints about data misuse.
- The Ministry should establish mechanisms for ongoing oversight and monitoring of compliance with the amended regulation. This may include appointing a regulatory body or commission responsible for enforcing data protection measures, conducting regular audits of telecom providers' data handling practices, and imposing penalties for non-compliance.

355 Kassouwi (n 182).
356 Section 27 of National Security Services
357 *Mofomobe Case* (n 161) paras 16 & 19.



CHAPTER 7

VULNERABLE AND MARGINALISED GROUPS IN THE DIGITAL AGE

7. VULNERABLE AND MARGINALISED GROUPS IN THE DIGITAL AGE

7.1 Digital inclusion and digital divide

In order for marginalised demographics, including women, children, individuals with disabilities, and rural communities, to fully reap the advantages of internet connectivity and realise their digital rights, it is essential to integrate them into the digital sphere. These groups possess an inherent right to access and utilise the internet, as articulated in Principle 37 of the 2019 ACHPR Declaration. This principle entails the significance of universal and equitable internet accessibility in the attainment of fundamental rights such as freedom of expression and access to information. Consequently, governments are mandated to implement measures to ensure the provision of internet access without discrimination, thereby enabling marginalised populations to effectively exercise their digital rights.[358] States should also ensure that marginalised groups enjoy the rights to freedom of expression and access to information on an equitable basis within the digital realm. Principle 11 of the ACHPR Declaration reinforces this obligation by stipulating that governments should enact policies to promote a diverse media landscape, thereby facilitating access to media outlets and other communication platforms for rural communities and other marginalised segments of society.[359] The following discussion aims to elucidate the digital discrepancies experienced by vulnerable and marginalised groups compared to other segments of society in Lesotho. Additionally, it seeks to explore initiatives directed towards digital inclusion for these groups.

7.1.1 Rural communities

In 2018, studies revealed a significant digital disparity within Lesotho, highlighting that around 83% of its rural population was devoid of internet access, while in stark juxtaposition, approximately 50% of urban residents enjoyed digital connectivity.[360] This digital reality is exacerbated by several contributing factors, such as the prohibitive cost of internet connectivity, limited literacy proficiency, the prevalence of English as the dominant language in online platforms over Sesotho, and the perceived lack of relevance of internet technologies to the socio-economic landscape of rural communities.[361] These conditions undermine the ability of rural populations to harness the transformative potential of digital technologies and fully exercise their rights to digital access and utilisation.

Recommendations

The following recommendations are proposed to facilitate enhanced inclusion of rural communities in the digital ecosystem.

- The government, in collaboration with stakeholders, should undertake measures to alleviate the financial barriers associated with accessing the internet.[362] This may involve implementing policies aimed at reducing internet subscription fees or providing subsidies for marginalised groups. Additionally, the government should prioritise initiatives that

358 Principle 37 (2) - (4) ACHPR 2019 Declaration.
359 Article 2 African Charter.
360 Africa Portal 'SADC not bridging the digital divide' https://www.africaportal.org/features/sadc-not-bridging-digital-divide/ (accessed 28 May 2023).
361 T Machone 'Preserving an open internet in Lesotho through a multi-stakeholder dialogue' *Open Internet for Democracy* 22 September 2022. https://openinternet.global/news/preserving-open-internet-lesotho-through-multi-stakeholder-dialogue (accessed 07 August 2023).
362 APAI (n 44) para 3.

ensure marginalised groups have free access to essential online information resources.

- Government entities and stakeholders should facilitate the development of internet content tailored specifically to the linguistic and practical needs of rural communities, particularly in the Sesotho language. Such content should address pertinent aspects of rural life, such as livestock registration procedures, thereby promoting digital literacy and engagement among rural populations.[363] By facilitating access to locally relevant digital resources, rural communities can better exercise their rights within the digital sphere and actively participate in technological advancements.

7.1.2 Women

In Lesotho, women constitute 50.7% of the population, while males account for 49.3%.[364] However, a gendered digital divide persists, with 36% of men and 31% of women engaging with internet technologies.[365] This divergence is exacerbated by the dearth of female representation in ICT education programs and the prevalence of low employment and literacy rates among women, thus constraining their exposure to the digital realm.[366] Furthermore, female enrollment in higher education institutions, particularly in fields inclusive of Science, Technology, Engineering, and Mathematics (STEM) or ICT-related disciplines, remains disproportionately low. Even among those who pursue such academic paths, computer science specialisations are seldom chosen by women. Remarkably, female leadership is conspicuously absent within Information Technology (IT) firms,[367] and similarly, women occupy few leadership roles within the media sector.[368] Moreover, this underrepresentation extends to the realm of internet governance, further marginalising women's voices and perspectives in shaping digital policy and regulation. These multifaceted challenges collectively compromise the digital rights of women in Lesotho, curtailing their access to information, freedom of expression in media channels, and broader digital rights.

The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) mandates governments to actively combat discrimination against women in all its manifestations and to concretely realise the principle of gender equality.[369] Moreover, the Protocol to the African Charter on Human and Peoples Rights on the Rights of Women in Africa provides that states should eliminate all forms of discrimination against women.[370] Additionally, the African Declaration on Internet Human Rights and Freedoms asserts that governments should adopt strategies to ensure the equitable and comprehensive participation of women in decision-making processes that shape the internet and its governance. Empowering women to achieve gender parity in online spaces is paramount.[371] Therefore, Lesotho should steadfastly strive towards realising this objective.

---

363 Machone (n 361).
364 Kemp (n 61).
365 Africa Portal (n 360).
366 Centre for Human Rights (n 2) 57.
367 World Bank *Lesotho Digital Economy Diagnostic* https://documents1.worldbank.org/curated/en/196401591179805910/text/Lesotho-Digital-Economy-Diagnostic.txt (accessed 28 May 2023).
368 MISA (n 65) 45.
369 UN General Assembly 'Resolution 34/180: Convention on the Elimination of All Forms of Discrimination against Women' (1979) https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/cedaw.pdf (accessed 09 August 2023).
370 African Union 'Protocol to the African Charter on Human and Peoples Rights on the Rights of Women in Africa' (2003) https://www.ohchr.org/sites/default/files/Documents/Issues/Women/WG/ProtocolontheRightsofWomen.pdf (accessed 11 August 2023).
371 AIR (n 44) 25.

Research indicates that women are disproportionately subjected to online violence,[372] including various forms such as threats, harassment, and discrimination.[373] As a result, women tend to self-censor and participate less on online platforms. This reality effectively undermines their constitutionally guaranteed right to freely express their opinions[374] and significantly impedes their rights to political engagement, including participation in public discourse and electoral processes.[375] This could be participation in public affairs or running for elections. The act of sharing women's images online without their consent affects the right to bodily integrity, human dignity and right to privacy. It is noted that the Declaration on the Elimination of Violence Against Women provides that states should condemn violence against women, and eliminate and punish, through legislation, acts of violence against women.[376]

Although the Penal Code does not explicitly address online violence, it criminalises the communication of a threat of death or physical harm through gesture, writing or words.[377] While the Code does not directly reference the online sphere, its provisions can be interpreted to include online threats. However, the Counter Domestic Violence Bill addresses online abuse of women in the online realm. The Bill, designed to safeguard victims of domestic violence, defines domestic violence to include acts causing emotional, physical, or sexual harm, which includes instances of technology-facilitated abuse.[378] The Bill does not, however, define technology abuse or how it can manifest. For the protection of women from online gender-based violence, the Computer Crime and Cyber Security Bill criminalises actions committed against women such as cyberbullying, harassment and distribution of intimate images without consent.[379] It also covers any offensive acts conducted under other Acts,[380] but conducted through a computer system or electronic device or electronic form. It is hoped that the enactment of this Bill will serve to combat online abuse and afford protection to women engaged in diverse sectors, including politics, journalism, and beyond.

Recommendations

The following recommendations are proposed to effectively enhance the protection of women in the digital age, promote gender equality in the digital sphere, and create a more inclusive and empowering environment for women's participation and leadership in technology and media industries.

- The government should develop and implement policy measures aimed at ensuring the full and meaningful inclusion of women in the online medium. These measures should address barriers to access, promote digital literacy among women, and facilitate a supportive environment that enables their active participation in digital spaces.
- The government should prioritise the development of policies aimed at increasing

372 MISA (2022) The State of Press Freedom in Southern Africa (2020-2021) 8.
373 Unpublished Dissertation S Mokapane 'Digital violence: an insight study on violence against women and girls online and the legal and institutional frameworks in Lesotho' unpublished dissertation, National University of Lesotho (2022) 36 https://repository.tml.nul.ls/bitstream/handle/20.500.14155/1716/Thesis-Digital-Mokapane-2022.pdf?sequence=1&isAllowed=y (accessed 13 August 2023).
374 Section 14 Constitution.
375 Section 20 Constitution.
376 Article 4 of UN General Assembly ' Resolution 48/104:Declaration on the Elimination of Violence Against Women' (1993) https://www.ohchr.org/sites/default/files/eliminationvaw.pdf (accessed 11 August 2023).
377 Section 34 Penal Code Act.
378 Section 3 (k) Counter Domestic Violence Bill.
379 Section 33 & 40 Computer Crime and Cyber Security Bill.
380 Such as the Sexual Offences Act 3 of 2003 https://gender.gov.ls/wp-content/uploads/2020/11/Lesotho-Sexual-Violence-Act-2003.pdf (accessed 12 August 2023).

opportunities for women to assume leadership roles in media houses and across various IT-related industries. This can be achieved through targeted initiatives such as mentorship programs, gender-sensitive recruitment policies, and support for women-owned tech enterprises.

- The government should devise measures and commit resources to promote women's participation in STEM (Science, Technology, Engineering, and Mathematics) and ICT-related higher education programs. This includes scholarships, grants, and outreach programs designed to encourage young women to pursue careers in these fields, thereby narrowing the gender gap in technology-related professions.
- To empower women in the digital age, the government should take proactive measures to ensure their equal access to information and freedom of expression through ICT platforms. This involves initiatives to bridge the digital divide, provide training in digital literacy and online safety, and create spaces for women to amplify their voices and advocate for their rights in online forums and public discourse.[381]
- The Counter Domestic Violence Bill should be expanded to explicitly address the issue of technology-facilitated abuse and harassment. This includes recognizing and defining various forms of technology abuse, such as cyberstalking, non-consensual distribution of intimate images, and digital surveillance, and incorporating provisions to protect victims and hold perpetrators accountable within the legal framework.

7.1.3 Children

In 2021, 30% of internet users in Lesotho were people aged 18 and below.[382] The UN Convention on the Rights of a Child (CRC)[383] and the African Charter on the Rights and Welfare of the Child (ACRWC),[384] define a child as anyone below the age of 18 years. Whereas children benefit from the use of the internet, they are exposed to online dangers as well. The dangers include sexual abuse on the internet and processing of their personal information which may lead to identity theft and other malicious uses. Consequently, there is a need to promote and protect children's human rights in the digital sphere.

The CRC, General Comment 25 on children's rights in relation to the digital environment, provides that states should ensure that all children have equal and effective, meaningful access to the internet.[385] States should have the best interests of a child in any action they take.[386] Thus in regulation and management of the internet, states should prioritise the best interests of a child such as rights to seek, receive and impart information, give due weight to their views and protect them from harm.[387] Further, the ACRWC mandates states to protect children from sexual exploitation and sexual abuse.[388] Sexual exploitations include inducing or encouraging children to engage in sexual activities such as the production of pornographic material and activities related to prostitution. Additionally, states should protect children from risks to their

381 APAI(n 44).
382 Pule (n 87).
383 Article 1 UN Convention on the Rights of a Child.
384 OAU 'African Charter on the Rights and Welfare of a Child'(1990) https://au.int/sites/default/files/treaties/36804-treaty-0014_-_african_charter_on_the_rights_and_welfare_of_the_child_e.pdf (accessed 11 August 2023).
385 General Comment 25 on Children's Rights in relation to the Digital Environment CRC/C/GC/25, para 09 https://digitallibrary.un.org/record/3906061?ln=en (Accessed 12 August 2023).
386 Article IV African Charter on the Rights and Welfare of a Child.
387 General Comment 25 (n 385) para 12.
388 Article 27 African Charter on the Rights and Welfare of a Child.

life, survival, and development.[389] Thus, they should take measures to protect children from risks relating to internet content or actions that include violence, sexual exploitation, suicidal incitement, cyberbullying and harassment to mention a few.[390]

Moreover, states should enable children to express their opinions, exercise freedom of thought, associate freely, and have their privacy protected and their right to education guaranteed[391] in the digital environment.[392] Thus, they should involve children in the development of internet policies and regulations.[393] The establishment of national protection systems such as helplines, imposition of obligations on digital service providers to report child-abusive material and criminalisation of dissemination of child pornography should be prioritised by states.[394]

It is noted that among the benefits of digital technology, it promotes children's right to health. Children find information on the internet for diagnostic and treatment purposes. The information assists them with their mental, sexual, physical, and reproductive health and counselling services. States should ensure that children have access to safe and secure health information. They should also advance research in the innovation of technologies that promote health.[395]

In securing the digital rights of children, Lesotho has enacted legislation that protects children from unlawful data processing. The DPA states that a data controller shall not process a child's personal information without prior parental consent.[396] An exception occurs when an institution processes the child's personal information in the performance of its legal duties relating to the child's protection or guardianship.[397]

Further, Lesotho's Computer Crime and Cyber Security Bill makes child pornography an offence. This offence refers to the production, procurement, possession, access to, or distribution of visuals that depict a child engaged in sexual acts through a computer system or show their sexual organs for sexual purposes.[398] The Sexual Offences Act criminalises child molestation, sexual abuse of a child and commercial sexual exploitation of children,[399] but it does not extend the offences to the digital forum. The Ministry of Social Development has established a Child Helpline that provides counselling and referrals, and links children to relevant services as a measure to protect against child abuse.[400] These measures attempt to protect the rights of a child in the online medium.

389 Article V African Charter on the Rights and Welfare of a Child.
390 General Comment 25 (n 385) para 14 & 82.
391 Articles VII-XI African Charter on the Rights and Welfare of a Child, 1990; Article 16 UN Convention on the Rights of a Child.
392 General Comment 25 (n 385) para 99-100.
393 General Comment 25 (n 385) para 16.
394 ACERWC 'Resolution NO.17/2022: Resolution of the ACERWC Working Group on Children's Rights and Business on the Protection and Promotion of Children's Rights in the Digital Sphere in Africa' https://www.acerwc.africa/sites/default/files/2022-10/Resolution%20No%2017%202022%20of%20the%20Working%20Group%20on%20Children%27s%20Rights%20and%20Business_0.pdf (accessed 12 November 2023).
395 General Comment 25 (n 385) para 93-98.
396 Sections 29 (a) and 36 (a) DPA.
397 Sections 34 (1) (d) DPA.
398 Section 32 Computer Crime and Cyber Security Bill. It complies with Article 9 of the Convention on Cybercrime.
399 Parts III & IV Sexual Offences Act.
400 N Velaphe 'Social Development re-launches child helpline Lesotho' *Government of Lesotho* https://www.gov.ls/social-development-re-launches-child-helpline-lesotho/ (accessed 12 August 2023).

There are no legislative measures or policies in Lesotho that indicate how content that threatens the survival and development of children may be monitored. Guardians or parents currently rely on measures provided by content providers such as YouTube parental controls.

Recommendations

The following recommendations are proposed to the state as the duty bearer to strengthen the protection of children in the digital age while strengthening their safe and constructive engagement with technology.

- The Ministry of Law and Constitutional Affairs should amend the Sexual Offences Act to explicitly address instances of sexual exploitation and abuse of children in digital spaces. This amendment will provide robust legal protection to children against digital sexual offences.
- The Ministry of Education should proactively develop comprehensive policies aimed at facilitating safe and responsible online behaviour among children. These policies should be integrated into educational curricula, empowering children with the knowledge and skills to navigate the digital landscape securely while upholding their rights.
- The Computer Crime and Cybersecurity Bill should be revised to include a wider range of offences pertinent to the digital realm. This includes but is not limited to, provisions addressing online incitement to self-harm, dissemination of violent content to minors, and instances of underage gambling, as outlined by the UN CRC General Comment No. 25.
- To safeguard children's interests in the digital sphere, the Ministry of Social Development should establish an independent body tasked with overseeing all internet-related activities concerning children. This body should ensure alignment with the principles of child welfare and participation, thereby ensuring that children's voices are heard and their digital rights upheld.
- The Ministry of Social Development should develop a comprehensive policy framework aimed at shielding children from exposure to harmful content on the internet. This policy should include measures for content moderation, parental controls, and educational initiatives to mitigate the risks associated with online content consumption.

7.1.4 Persons with Disabilities

Persons with disabilities (PWDs) are entitled to equitable access to and utilisation of the internet, a fundamental aspect of their rights. States bear a particular responsibility to address the unique needs of PWDs and to institute measures to prevent discrimination in the enjoyment of human rights within the digital realm. The Convention on the Rights of Persons with Disabilities (CRPD) mandates that states should actively uphold and promote the human rights of individuals with disabilities, without any form of discrimination.[401] Central to this consideration is the state's obligation to ensure that PWDs enjoy equal access to ICTs and the internet as their nondisabled counterparts.[402] States are also encouraged to implement targeted interventions to guarantee the accessibility of rights such as freedom of expression and the freedom to seek, receive, and disseminate information, across all modes of communication, including the internet.[403]

401 UN 'Convention on the Rights of Persons with Disabilities' (2006) https://www.ohchr.org/sites/default/files/Ch_IV_15.pdf (accessed 12 August 2023).
402 As above.
403 Article 21 Convention on Rights of Persons with Disabilities ; See Principle 7 of the ACHPR 2019 Declaration.

Several impediments hinder PWDs from accessing ICTs. These include a deficiency in the requisite skills to effectively utilise ICTs, compounded by the exorbitant costs of digital devices tailored to accommodate their specialised needs for sustenance. Additionally, the dearth of specialised software and hardware catering to the unique requirements of PWDs exacerbates accessibility challenges. Moreover, a lack of awareness regarding the advantages of ICTs further impedes their integration into the lives of PWDs.[404] Barriers are also compounded by factors such as digital content presented in non-accessible formats, limited availability of affordable assistive technologies, and restrictions on the utilisation of digital devices by children with disabilities within educational settings.

The UN CRC General Comment 25 provides that states shall take measures to remove barriers faced by children with disabilities with regard to the digital environment.[405] They should ensure access to content in accessible formats; avail affordable assistance technologies; remove policies that discriminate against PWDs; train disabled people and their families on skills to use digital technology; promote technological innovations with universal access so that they are accessible to PWDs without alteration; and engage PWDs in policy-making meant to realise their digital rights. Further, the states should identify risks faced by PWDs such as sexual exploitation, and take measures to protect PWDs from the risks, but should be careful not to be overprotective and exclude them from the enjoyment of digital rights.[406] Additionally, in accordance with UN General Comment 4, states are mandated to uphold the right to education for disabled persons through the design and implementation of inclusive education systems. This necessitates the development and deployment of innovative technologies conducive to enhanced learning experiences, ensuring accessibility for children with disabilities, and facilitating the integration of assistive technology within educational settings.[407]

In the pursuit of advancing digital rights, the Persons with Disability Equity Act[408] acknowledges that communications directed towards PWDs should be accessible in any format, including through accessible ICTs. In alignment with this commitment, Vodacom Lesotho recently established a digital library catering to visually impaired individuals at the Lesotho National Library, aimed at facilitating their right to access information.[409] While the Act largely aligns with the provisions of the CRPD, it notably falls short of extending these rights to the online domain. However, the legislation does establish a Persons with Disability Advisory Council, mandated to provide counsel to the government on disability-related matters.[410] Among its multifaceted responsibilities, the Council is tasked with monitoring the human rights status of PWDs, advising the Human Rights Commission, reporting violations against PWDs, promoting research on disability issues to inform policy formulation, and undertaking initiatives to promote the rights of PWDs.[411] Consequently, the Council possesses the potential to significantly influence the formulation of government policies conducive to advancing the digital rights of PWDs.

404 P Nikolaidis & D Xanthidis 'People with disabilities in the Digital Era: A basic review of the policies and technologies' in X Zhuang *Recent Advances in Computer Sciences* (2015) 228-233.
405 General Comment 25, para 84.
406 General Comment 25 (n 385) para 90-92.
407 General Comment 25 (n 385) para 8, 21
408 Persons with Disability Equity Act 2 of 2021 https://media.lesotholii.org/files/legislation/akn-ls-act-2021-2-eng-2021-03-12.pdf (accessed 05 June 2023).
409 S Nkhasi 'Disability Lesotho' (2021) 9 *Lesotho National Federation of Organisations of the Disabled* http://www.lnfod.org.ls/uploads/1/2/2/5/12251792/disability_lesotho_dec_2021__1_.pdf (accessed 11 August 2023).
410 Section 4 Persons with Disability Equity Act.
411 Section 6 Persons with Disability Equity Act.

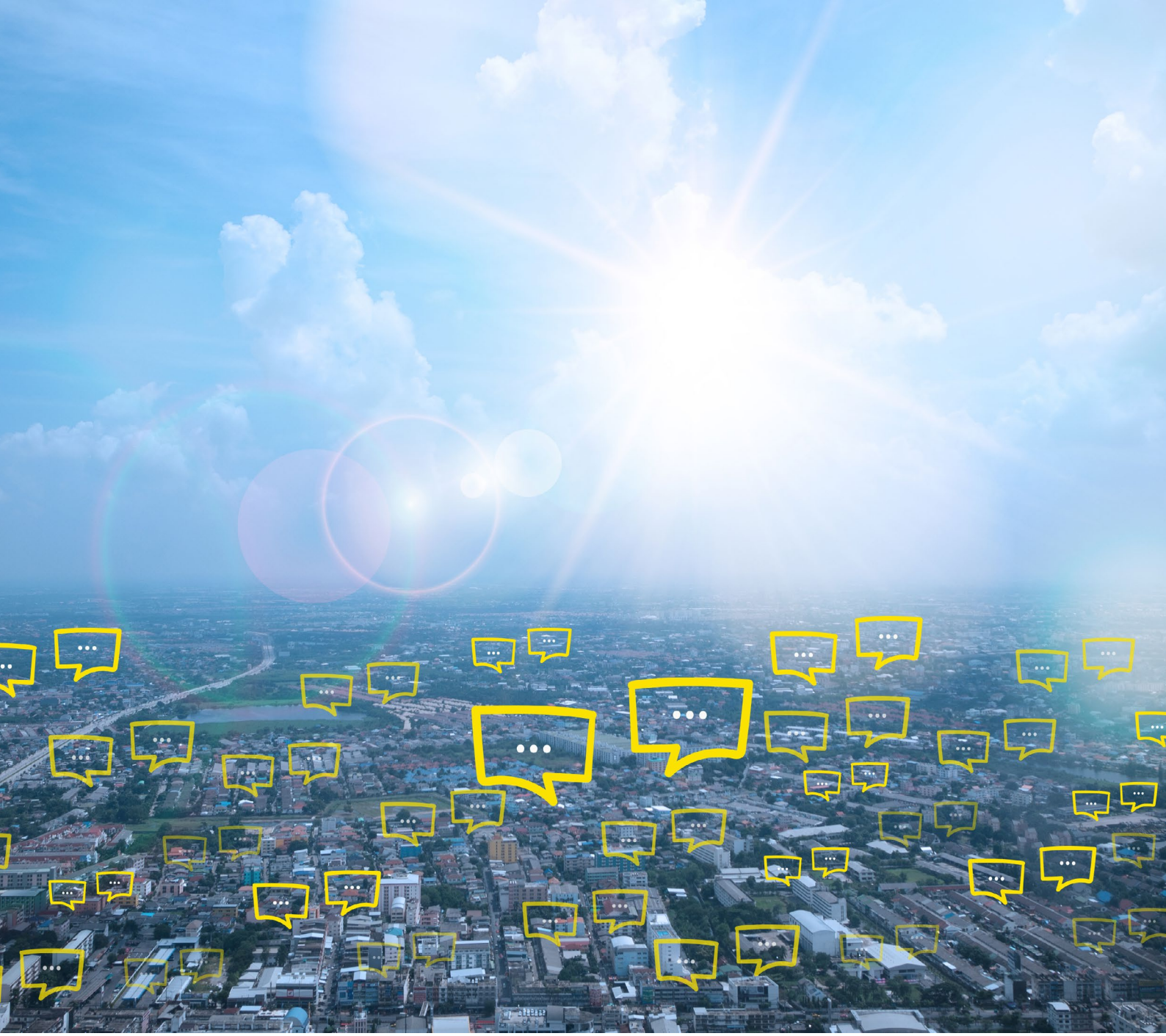
Conversely, while the Sexual Offences Act criminalises sexual acts involving or in the presence of disabled individuals[412] it does not extend these provisions to the digital realm.

Recommendations

The following recommendations are proposed for duty-bearers and other stakeholders to consider in promoting digital inclusion for persons with disabilities in the digital environment:

- Facilitate digital literacy for PWDs and their families to enhance their skills and empower them to navigate the digital landscape effectively.
- Develop comprehensive education policies that prioritise the integration of assistive technologies in learning environments, thereby nurturing inclusive learning opportunities for PWDs and upholding their right to education.
- Address barriers to access to Information and Communication Technologies (ICTs) by implementing measures such as the provision of assistive devices and ensuring the accessibility of digital platforms and services for PWDs.
- Promote collaboration between stakeholders and innovators to develop specialised technologies tailored to the unique needs of PWDs, similar to the commendable initiative undertaken by Vodacom, thereby expanding access to ICT information and services for PWDs.
- Promote the meaningful participation of PWDs in policy-making processes related to digital inclusion, ensuring that their perspectives and needs are adequately represented and prioritised in decision-making initiatives.

412 Section 15 Sexual Offences Act 2003.



CHAPTER 8
THE DIGITAL ECONOMY IN LESOTHO

8. THE DIGITAL ECONOMY IN LESOTHO

The digital economy represents an essential avenue for advancing Lesotho's economic development aspirations, holding substantial promise for transformative growth. Hence, the development of a digital ecosystem in accordance with established human rights principles is crucial for maximising this potential and fulfilling the nation's economic objectives. At its core, the digital economy operates through the utilisation of digital technologies, particularly the internet, facilitating the exchange and dissemination of information and knowledge. Thus, the digital economy encompasses the multifaceted processes of information generation, processing, and transmission. The proposed SADC Model Law for Digital Economies reiterates the need for states to capitalise on the advantages afforded by the digital economy while concurrently safeguarding the fundamental rights of their citizens and mitigating associated risks inherent in developmental pursuits.[413] Consequently, the promotion and protection of rights pertaining to access to information, freedom of expression, privacy, and data protection emerge as paramount considerations within the digital landscape, as expounded upon earlier within this report.

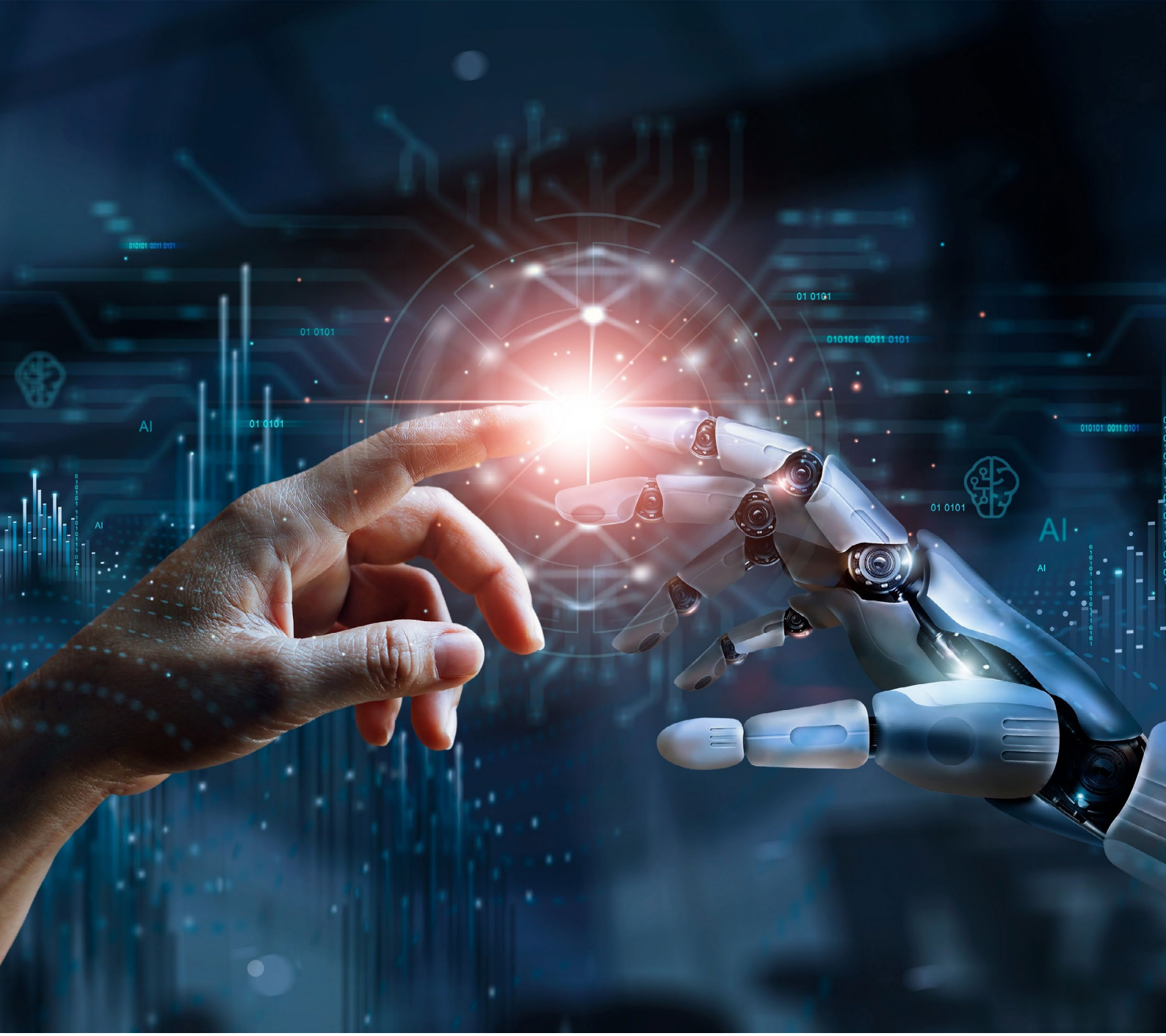
Lesotho's digital economy hinges on the acknowledgment and enforcement of open internet access, aligned with the principle of network neutrality. This entails the equitable treatment of data traversing the internet, devoid of discriminatory practices, 'according to user, content, site platform, application, type of attached equipment and modes of communication.'[414] Such practices ensure the extensive exchange of information and communication without bias or impediments. Embracing open standards not only cultivates an environment conducive to innovation but also promotes a healthy competition within the digital realm.

The Constitution of Lesotho upholds the principle of network neutrality as an extension of its safeguarding of freedom of expression.[415] It states that a person should not be hindered from enjoying their freedom of expression, and should be able to communicate their ideas without hindrance. In other words, a person may communicate through the internet or different digital mediums without any impediment. . In alignment with the promotion of network neutrality, the Electronic Transactions and Communications Bill of 2022 within the legislative framework of Lesotho guarantees the legal recognition and validity of electronic communications in the realm of electronic commerce.[416] This legislation defines electronic communication comprehensively, including data messages transmitted through electronic mail, Short Message Services (SMS), mobile communications, videos, audio recordings, or analogous means.[417] It also recognises the right to access information and data privacy by mandating that providers of online services or products furnish comprehensive information regarding their offerings, including specifications, costs, identity verification, security protocols, and privacy policies concerning payments and personal data.[418] Concurrently, the Consumer Protection Bill has provisions safeguarding the rights of information consumers and ensuring the protection of their privacy with regards to personal information divulged during transactions.[419]

413 G Razzano 'SADC Parliamentary Forum Discussion Paper: The Digital Economy and Society' (2020) *Research ICT Africa* 2.
414 APAI (n 44)16.
415 Section 14 Constitution.
416 Section 6 Transactions and Communications Bill.
417 Section 2 Electronic Transactions and Communications Bill.
418 Section 31 Electronic Transactions and Communications Bill. The Bill adopts the SADC Model Law.
419 Section 4 Consumer Protection Bill.

Vodacom Lesotho (VCL) and Econet Telecom Lesotho (ETL) dominate the mobile telecommunications landscape in Lesotho, functioning as the primary Mobile Network Operators (MNOs), while facing limited competition from Internet Service Providers (ISPs) like ComNet and Leo. This lack of competitive market dynamics exacerbates the prevalence of high-value bundle services, perpetuating structural pricing disparities that disproportionately impact economically disadvantaged communities. Notably, the pricing structure exhibits biases against lower-income demographics; for instance, post-paid data services are priced more favourably compared to their prepaid counterparts. Consequently, individuals with limited financial means are compelled to purchase smaller data bundles at higher rates relative to larger bundles. Moreover, the prohibitive costs associated with acquiring devices further exacerbate socioeconomic disparities within the community, exacerbating the divide between affluent and marginalised segments of society.[420] Such circumstances run counter to the principles of net neutrality and consequently encroach upon individuals' rights to equitable enjoyment of human rights without discrimination.

420 World Bank group 'Lesotho Digital Economy Diagnostic' (2020) 10 https://documents1.worldbank.org/curated/ar/196401591179805910/Lesotho-Digital-Economy-Diagnostic.docx (accessed 02 January 2024) .



CHAPTER 9
NEW AND EMERGING TECHNOLOGIES

9. NEW AND EMERGING TECHNOLOGIES

The landscape of cutting-edge technologies continues to evolve, showcasing advancements such as biometrics, facial recognition, AI, and robotics. These innovations wield transformative power over both the economy and society within a state. They hold promise in revolutionising, for instance, education by supporting enhanced learning experiences, strengthening health services, and optimising financial systems. However, alongside their potential benefits, these emerging technologies also raise concerns about encroachment on privacy, freedom of expression, and other digital rights. Therefore, effective regulation is essential to ensure their responsible deployment and mitigate potential adverse consequences.

The ACHPR Resolution accentuates the exigency of initiating an exhaustive inquiry into the confluence of human and peoples' rights vis-à-vis the advancements in AI, robotics, and other nascent technologies throughout Africa. It reiterates the prospective capacity of these innovations to ameliorate instances of human rights transgressions. The resolution mandates that member states adhere to the precepts enshrined in the African Charter and other relevant instruments, thereby ensuring that the deployment of such technologies aligns seamlessly with established human rights standards. It also enjoins states to promulgate robust legislative frameworks and guidelines to effectively regulate the ethical and equitable deployment of these technologies.

Lesotho strategically leverages emergent technologies to realise the objectives outlined in its National Strategic Development Plan (NSDP II).[421] At the core of this strategy lies the emphasis on innovation and technological advancement, acknowledged for its potential to generate employment opportunities, strengthen various facets of economic growth, and mitigate poverty. Specifically, sectors dedicated to technological production hold promise for catalysing the advancement of Small, Medium, and Micro Enterprises (SMMEs). Concurrently, the NSDP II reiterates the importance of upholding and safeguarding the human rights of all individuals, with this commitment as a focal priority area.

Lesotho has initiated the integration of biometric authentication in its SIM card registration process. Governed by the Communications Regulations, this framework authorises the registration of SIM cards by capturing pertinent details from the identity cards or licences of users. As previously highlighted, however, the implementation of such regulations presents concerns regarding indiscriminate surveillance and potential encroachments upon the right to privacy.

Lesotho has embraced the integration of artificial intelligence (AI) across various sectors of its economy, notably in agriculture, healthcare, and industry. In the manufacturing sphere, for instance, automated machinery has been deployed to undertake repetitive tasks previously executed by human labourers within factory settings.[422] Similarly, within the mining sector, AI technologies regulate the transportation logistics of trucks within mining compounds. Furthermore, AI applications have permeated electronic commerce operations in Lesotho. Beyond industrial contexts, AI innovations are instrumental in enhancing agricultural

421 Genesis *Formulating Lesotho's National Digital Transformation Strategy* https://www.genesis-analytics.com/projects/strategy-for-digital-transformation-across-all-of-lesotho-government#:~:text=Lesotho's%20digital%20economy%20holds%20immense,developing%20a%20national%20payments%20switch (accessed 11 August 2023).

422 JF Arinez et al 'Artificial Intelligence in Advanced Manufacturing: Current Status and Future Outlook' 2020 142 *Journal of Manufacturing Science and Engineering*.

productivity and operational efficiency, thereby catalysing economic growth.[423] Additionally, AI facilitates advancements in healthcare accessibility by enabling self-diagnostic capabilities and early-stage healthcare provision, thus augmenting public health outcomes.[424]

Furthermore, within the educational and research domains in Lesotho, internet users utilise Chat Generative Pretrained Transformer (ChatGPT) as a tool for knowledge acquisition and scholarly inquiry. ChatGPT, an AI-driven conversational agent, harnesses natural language processing algorithms to simulate human-like interactions. Its functionalities encompass responding to queries, conducting research, drafting essays, emails, and social media content, as well as crafting persuasive discourse.[425] While ChatGPT holds promise in augmenting educational pursuits, cautious consideration is warranted regarding its potential to engender overreliance among young learners. Excessive dependence on such technology may impede children's cognitive maturation, thereby necessitating safeguards to uphold their rights to life and holistic development.

The impact of AI on the employment landscape in Lesotho manifests predominantly through heightened redundancy, as human labour is supplanted by AI-driven systems. This phenomenon presents a conundrum vis-à-vis the right to employment, enshrined within both the African Charter and the national Constitution.[426] Conversely, the proliferation of emergent technologies engenders job creation within the technology sector, notably in domains such as programming, robotics, and data analysis. Individuals possessing expertise in developing assistive technologies, including AI-powered chatbots, natural language processing proficiency, digital marketing acumen, and logistics management, are poised to benefit from burgeoning employment opportunities. Consequently, those equipped with AI-related proficiencies stand to secure and sustain employment, thereby exacerbating disparities in the labour market, to the detriment of the principle of equal enjoyment of human rights without discrimination.[427]

In light of the dynamic shifts within the labour landscape, workers should undergo continuous skills acquisition to ensure their continued relevance within the evolving job market. The Constitution mandates the formulation of policies on technical training and vocational guidance, thereby affording all citizens equitable opportunities for gainful employment.[428]

Recommendations

The following recommendations are proposed for governmental consideration to facilitate the responsible integration of cutting-edge technologies:

- The government should formulate comprehensive policies focused on advancing education and training initiatives to equip individuals with the requisite skills necessary for navigating the disruptions within the job market precipitated by new and emerging

423 Ministry of Communications, Science and Technology Science, Technology and Innovation Review and Technology Needs Assessment for Lesotho (2022) 59 https://www.un.org/technologybank/sites/www.un.org.technologybank/files/lesotho_tna_report_final_6_may_2022.pdf (accessed 11 October 2023).

424 MY Shaheen 'Applications of Artificial Intelligence (AI) in healthcare: A review' (2021) https://www.scienceopen.com/hosted-document?doi=10.14293/S2199-1006.1.SOR-.PPVRY8K.v1 (accessed on 08 November 2024).

425 A Hetler 'What is Definition ChatCPT. [Online] Available from https://www.techtarget.com/whatis/definition/ChatGPT (Accessed 12 August 2023).

426 Article 15 African Charter.

427 Article 2 African Charter.

428 Section 29 Constitution.

technologies. This proactive approach ensures that individuals remain adept and competitive within the evolving labour landscape.

- The Ministry of Communications, Science, and Technology, in collaboration with the Ministry of Education, should devise and implement robust policies aimed at safeguarding against the potential adverse effects stemming from the indiscriminate and excessive utilisation of emerging technologies within educational institutions. These policies serve to mitigate risks and uphold the integrity of educational environments.
- The Ministry of Communications, Science, and Technology, in conjunction with the Ministry of Education, should initiate programs geared towards educating parents and guardians on the judicious selection and supervised utilisation of technologies conducive to child education. By empowering parents and caregivers with pertinent knowledge and guidance, the responsible integration of technology within educational settings can be ensured, ensuring optimal learning experiences for children.

CHAPTER 10
CONCLUSION

10. CONCLUSION

In conclusion, this report highlights the intrinsic importance of human rights in the digital age, affirming their vital role in safeguarding human dignity. It emphasises the obligations of states as duty bearers to adhere to established international human rights laws and standards to ensure the protection and promotion of these rights. The report reiterates that human rights are universal and inalienable, extending equally to all individuals, whether offline or online. Encouragingly, Lesotho has begun recognising the significance of digital rights, marking a positive step forward. Despite challenges such as limited internet access and the need for more robust protection of online rights, implementing the recommendations outlined in this report promises to advance the cause of human rights in the digital sphere within Lesotho, promoting a more inclusive and rights-respecting environment for all.


UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA


Centre for
Human Rights
UNIVERSITY OF PRETORIA


ADVANCING RIGHTS
IN SOUTHERN AFRICA
ARISA


Transformation
Resource Centre


Internews
Local voices. Global change.