TECH HIVE ADVISORY

The intersection of the right to freedom of expression online and protection of personal information in Botswana, Ethiopia, Kenya, and Nigeria.

Executive Summary

This report focuses on the intersection of the right to freedom of expression online and the protection of personal information in four African countries: Botswana, Ethiopia, Kenya, and Nigeria. The report is divided into five major parts, including the introduction and conclusion. The first introduces the report, while the second part focuses on the normative standards concerning the right to freedom of expression online and protection of personal information under the United Nations and the African human rights systems.

Under both systems, it focused on the applicable provisions of the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples' Rights (African Charter). It noted that both rights are not only protected as stand-alone rights under both systems; their intersections, namely media freedoms, the 'right to be forgotten' and encryption and anonymity, are also protected. Therefore, States party to both the ICCPR and the African Charter, including Botswana, Ethiopia, Kenya and Nigeria, have an obligation to protect both rights separately and jointly.

The third part examines the state of both rights and their intersections in Botswana, Ethiopia, Kenya and Nigeria. In doing this, each country report is divided into four major sections save for Kenya, which includes a section on major highlights of the report.

For Botswana, the first part introduces the landscape on the right to freedom of expression online and protection of personal information. The second section of the Botswana report focuses on the constitutional guarantee, laws and major incidents like arrests and court cases that impact the right to freedom of expression, especially online in Botswana. It noted that while the right to freedom of expression has fared relatively well in the last few years, there are a number of laws that pose threats to the enjoyment of the right. The laws include the provisions of sections 59(1) and 93 of the *Penal*

Code, Section 18 of the *Cybercrime and Computer Related Crimes Act of 2018*, Sections 3 and 6 of the *Media Practitioners Act of 2008,* which provide for offences of alarming publications, criminalisation of insulting language, offensive communications online and the need for registration of media practitioners respectively.

The third section of the report considered the status of the protection of personal information in Botswana. It noted that while there is a constitutional guarantee on the right to privacy, the most proximate law on the right, the *Data Protection Act,* has not been implemented. It also noted the right to erasure and encryption as intersections of the right to freedom of expression and protection of personal information in Botswana. The final section concludes.

The first section of the report on Ethiopia also introduces both rights: freedom of expression online and protection of personal information. The second section analyses the constitutional guarantees under the FDRE Constitution, the laws and major incidents that impact the right to freedom of expression online in Ethiopia. It noted that various laws like *Proclamation No. 590/2008 of 2008, Hate Speech and Disinformation Proclamation No.1185/2020, draft Computer Crimes Proclamation of 2020* were generally in violation of various aspects of article 19 of the ICCPR on the right to freedom of expression.

The third section considered the status of protection of personal information in Ethiopia. It highlighted a number of laws that impact the right but notes that Ethiopia has yet to have a substantive data protection law. It also noted that with the gap created by such unavailability, the government continues to carry out various surveillance activities against human rights defenders and activists in the country. It also highlights the 'right to be forgotten', encryption and communications surveillance as major intersections of both rights. The final part concludes.

The Kenyan Report is similarly structured but with an additional section of its major highlights. The first section introduces the landscape of both rights in Kenya. In contrast, the second section focuses on the constitutional provisions, laws and major incidents concerning the right to freedom of expression online. Despite the constitutional guarantee and Kenya's obligations to protect the right under international human rights law, various provisions like Section 13 of the *National Cohesion and Integration Commission (NCIC) Act,* sections 22 and 23 of the *Computer Misuse and Cybercrimes Act,* section 16A *of Defamation Act,* and Section 84d *of the Kenya Information and Communications Act, (KICA) 1998* pose challenges in varying degrees to the right to freedom of expression online.

The third section of the report on the protection of personal information is also similar to the previous section as it finds that the right may be under threat in Kenya. For example, while the Data Protection Act is in force in Kenya, it is slow in terms of implementation, thereby creating a gap in the protection of personal information. It also noted that the energy of the Government of Kenya to collect and use personal information is not matched with the policy gaps and human rights concerns on the right to privacy. Concerning the intersection of both rights, it noted that in Kenya, journalistic exception, it also noted that both rights intersect in the areas of journalistic exception, right to rectification and erasure and encryption and anonymity. An additional section provides a highlight of the report, and the final section concludes.

Nigeria's report is also divided into four main sections. The first section introduces and the second section analyses the right to freedom of expression online by examining the constitutional provision, laws and major incidents that impact the right. It noted that despite the constitutional guarantee of the right, various sections of the *Penal Code*, *Cybercrimes Act* and other proposed laws like the

Protection from Internet Falsehood and Manipulations Bill, the *National Commission for the Prohibition of Hate Speeches bill*, and a host of other violations pose huge threats to the right to the freedom of expression online in Nigeria.

The third section examines the status of the protection of personal information in Nigeria. It noted that several laws impact such protection, including the *National Data Protection Regulation of 2019, Freedom of Information Act of 2013*, *Credit Reporting Act of 2017*, *National Health Act of 2014*, *National Identity Management Commission Act of 2007*, and the *Child Rights Act of 2013*. It noted that there are numerous challenges posed to the right into the allegations of arbitrary interference with the right to privacy by the government. It also noted that both rights intersect in the areas of journalistic exception, right to rectification and erasure and encryption and anonymity. The final section concludes on the need for more protection of both rights separately and jointly.

The fourth part of the report focuses on the major recommendations for each country based on their status of compliance with international human rights standards highlighted in the first part. The recommendations generally note that there is a need for legal reforms spearheaded by the States concerning basic digital rights in the country assessed. These legal reforms are mainly on the need for the governments to amend the relevant laws and ensure the enactment of rights-respecting ones. It also notes that the government must desist from arbitrary use of state powers that impact both rights.

In terms of the trends common to each country, the report finds that each country:

(a) Has constitutional guarantees and obligations under international human rights law to protect the rights to freedom of expression online and protection of personal information;

(b) Has various laws that negatively impact the rights to freedom of expression online and protection of personal information;

(c) Has major incidents in which State actors are the main violators of the right to freedom of expression online and protection of personal information;

(d) Needs urgent interventions of rights-respecting and inclusive laws and policies concerning the right to freedom of expression online and protection of personal information; and

(e) Has at least an intersection of the right to freedom of expression online and protection of personal information, including journalistic exception, encryption and anonymity, right to erasure and rectification, and communications surveillance.

In the final part, the report concludes in general; the need to protect media freedoms, ensure rights-respecting policies concerning the 'right to be forgotten and guarantee encryption and anonymity as essential aspects of the intersections of the right to freedom of expression online and protection of personal information features prominently in the report.

Contributors

Tomiwa Ilori coordinated the research report and prepared the first and second parts on the introduction and normative frameworks. He is a doctoral researcher at the Centre for Human Rights, Faculty of Law, University of Pretoria, where he works with the Expression, Information and Digital Rights Unit. He has research and public policy interests on how digital technologies impact human rights.

Senwelo Modise authored the country report on freedom of expression online and data protection in Botswana. She is a practising attorney at Botlhole Law Group [In Association with Neill Armstrong], a corporate and commercial law firm where she leads the Technology, Media and Telecommunications division. She specialises in technology law and is a subject matter expert in privacy, data protection and cybersecurity. In addition, she is interested in blockchain, digital health, fintech, artificial intelligence, electronic evidence, digital rights, and technology to improve efficiencies in legal practice.

Sigi Waigumo Mwanzia authored the country report on the status of the freedom of expression online and data protection in Kenya. She is a Digital Programme Officer at ARTICLE 19 Eastern Africa, where she leads the Digital portfolio focusing on freedom of expression online, data protection and privacy, and Internet access and affordability, amongst others. She is interested in the intersection between law, human rights, policy, and digital technologies and their contribution to national, regional, and international development.

Yohannes Eneyew Ayalew contributed the Ethiopian context of the report. He is a PhD Candidate at the Faculty of Law, Monash University in Australia. He is looking at balancing the freedom of expression and privacy on the internet under the African human rights system—his research interest spans the areas of public international law and human rights in the digital age.

Ridwan Oloyede co-authored the Nigerian chapter of the report. He is the Co-Founder of Tech Hive Advisory, where he leads the technology policy team. Ridwan advises on the global aspects of cybersecurity policy, data protection and privacy laws, digital health and digital ethics. He is also a policy analyst who has contributed to legislative processes. Ridwan is a Fellow of Information Privacy with the International Association of Privacy Professionals (IAPP) and a Research Fellow at the African Academic Network on Internet Policy.

Musa Omayi Sandra contributed to the Nigerian chapter of the report. She is a Tech Policy and Research Associate at Tech Hive Advisory. She has an interest in exploring the development of data protection and digital rights in Nigeria and globally.

Favour Borokini co-authored the Nigerian chapter of the report. She is a technology policy researcher with a law background from Nigeria. In her role as Data and Digital Rights Researcher with Pollicy, a Ugandan civic technology not-for-profit, she researches some knotty topics related to technology-facilitated violence against women and the widespread impact of subsisting and emerging technologies on social justice and equality. She also works as a Content Writer with Ethical Intelligence, an AI Ethics consulting firm and various research groups on data protection regulation and healthcare delivery. She is currently an Affiliate with The Future Society.

Copy editing

Latifah Salaudeen

The intersection of the right to freedom of expression online and protection of personal information in Botswana, Ethiopia, Kenya, and Nigeria.

Published by

TECH HIVE ADVISORY

Supported by

OMIDYAR NETWORK™

Design and Layout by

boldfusion

September 2021

Acknowledgement

This research report is carried out with the support of Omidyar Network. We thank Tomiwa Ilori, Yohannes Ayalew, Sigi Mwanzia, Senwelo Modise, Favour Borokini, Sandra Musa and Ridwan Oloyede for their valuable contributions. We also thank the copy editor, Latifah Salaudeen, the design team at Bold Fusion, and every other person that worked on the report for their input.

Table of Contents

PART 3

3. Country Report

KENYA

3.3. Introduction

While the protection and promotion of the right to freedom of expression have had a long and chequered history in Kenya, the prioritisation of the right to data protection was not properly protected through a stand-alone law until 2019. Kenya's transformative 2010 Constitution guarantees the rights to information and communications privacy and freedom of expression, both online and offline.[1] In addition to this, Kenya has ratified various international and regional instruments and treaties guaranteeing the right to freedom of expression and informational privacy. The ICCPR and the African Charter form part of Kenya's laws by virtue of Article 2 (6) of the 2010 Constitution. The Universal Declaration, which has attained the status of international customary law, also forms part of Kenya's laws under Article 2 (5) of the 2010 Constitution.

Kenya also ratified the African Charter on the Rights and Welfare of the Child (ACERWC) (1990), with Article 10 of the ACERWC explicitly protecting children's privacy against arbitrary and unlawful interferences. In 2018, Kenya ratified the African Continental Free Trade Area Agreement (AfCFTA), which, according to its Article 15 (a)(ii)) requires States to ensure 'the protection of the privacy of individuals about the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.' Notably, Kenya has not ratified the African Union Convention on Cybercrimes and Personal Data Protection (AU Convention).

While not binding on Kenya, soft law instruments such as the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa (the revised Declaration) and the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa establish guiding standards for the respect, protection and fulfilment of human rights. Kenya is also a member of the Freedom Online Coalition (FOC), where it is committed to promoting Internet freedom.

Despite these international and regional commitments and the transformative nature of the 2010 Constitution, Kenya's promotion of freedom of expression online has been typified by both standard-setting progression and rights-violating regression. Instructively, Kenyan courts have delivered positive pronouncements and struck down unconstitutional provisions for suppressing the right to freedom of expression, including provisions in the Penal Code. Despite this, Parliament has reintroduced some of these provisions, including criminal defamation. Problematically, many laws are not aligned with the 2010 Constitution and the general rules of international law and rely on disproportionate civil and criminal sanctions used by state agents to harass and intimidate targeted

[1] Constitution of Kenya <Kenya Law: The Constitution of Kenya> (2010).

online users. In effect, this situation has a 'chilling effect' on the right to freedom of expression online in Kenya.

On data protection, Kenya's *Data Protection Act* (DPA) 2019 was enacted in November 2019, but the enforcement of this law has been wanting with Kenya's first Data Protection Commissioner only being appointed in November 2020. In effect, this meant that the collection and processing of personal data, including sensitive health data, by State and non-State actors was unsupervised for one year. At an operational and functional level, many commentators note that Kenya's data protection authority lacks independence and autonomy and cannot properly oversee the protection of personal information and freedom of expression in Kenya.[2]

The right to freedom of expression online and data protection are mutually reinforcing and have the same level of importance under the Bill of Rights, i.e., no right is superior to the other. Some of the areas where these two rights intersect, demanding a proper balance between these co-equal rights, is by incorporating specific exemptions for journalistic, academic, artistic, literary and other cultural purposes in data protection laws, the right to rectification and erasure and encryption and anonymity.[3] However, as explored below, these intersections have not been adequately protected, especially as required under international human rights law.

When examining these and other concerns in detail, the report first documents the constitutional and legal status of the right to freedom of expression and data protection in Kenya. This is complemented by a breakdown of any major incidents like policy implementation, court cases, violations, forward-looking practices affecting the protection, promotion and fulfilment of these two rights. Building on this information, the report then identifies where freedom of expression and data protection intersect in Kenya. Finally, the report identifies key highlights before concluding. This report does not cover all the laws affecting freedom of expression and data protection; however, it exercised discretion and prioritised laws, policies, and issues that best reflect the country's situation.

3.3.1.Status of the right to freedom of expression online in Kenya

- ***Constitutional Provisions***

In Kenya, the right to freedom of expression is not only a fundamental enabler of other human rights, including media freedom and access to information. However, it is also the cornerstone of multi-party democracy. The right to freedom of expression for every person, online and offline, is primarily guaranteed under Article 33 of the 2010 Constitution. This provision states that:

"

> Every person has the right to freedom of expression, which includes—
>
> (a) freedom to seek, receive or impart information or ideas;
> (b) freedom of artistic creativity; and
> (c) academic freedom and freedom of scientific research.

"

In addition, this right is not absolute; the State can apply permissible limitations under exceptional circumstances. Under Article 33(2) and (3) of the 2010 Constitution, the right to freedom of

[2] ARTICLE 19 Eastern Africa, the Kenya ICT Action Network, Pollicy, 'Covid-19 surveillance in Kenya and Uganda is reducing people's rights' (2021) <https://www.Article19.org/covid-19-reduced-peoples-rights-in-kenya-and-uganda/> accessed 26 April 2021.
[3] ARTICLE 19, Rwanda: Draft data protection bill must incorporate freedom of expression and information safeguards < Rwanda: Draft data protection bill must incorporate freedom of expression and information safeguards - ARTICLE 19>, (2021) accessed 16 June 2021.

expression does not extend to 'propaganda for war, incitement to violence, hate speech, or advocacy of hatred.'[4] Further, the importance of 'respect' under Article 33(3), 2010 Constitution reveals the competing and conflicting nature of the right to freedom of expression with other individuals' rights and reputations. Similarly, Article 24 of the 2010 Constitution permits certain rights to be limited by law. However, this limitation must satisfy strict conditions and tests and be 'reasonable and justifiable in an open and democratic society.'

- ***Other Laws***

Some colonial-era and post-2010 Constitution laws interfere with the proper enjoyment of the right to freedom of expression, both online and offline, in Kenya. These include laws on hate speech, defamation, false publication, amongst others.

Hate Speech: The National Cohesion and Integration Commission (NCIC) Act

The National Cohesion and Integration Commission (NCIC) Act builds on the express prohibition of hate speech under the 2010 Constitution in Kenya. Generally, even though the term 'hate speech' has not been defined under conventional international law, various mechanisms have grappled with its meaning, but held that this term does not include broad terms including 'ridicule' or 'justification.'[5] Section 13, NCIC Act defines hate speech as speech which is,

threatening, abusive or insulting or involves the use of threatening, abusive or insulting words or behaviour commits an offence if such person intends thereby to stir up ethnic hatred, or having regard to all the circumstances, ethnic hatred is likely to be stirred up.

Hate speech under the NCIC Act is defined by reference to 'ethnic hatred', which means 'hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.' Here, any person who 'uses threatening, abusive or insulting words or behaviour, or displays any written material', or 'publishes or distributes written material' or 'presents or directs the performance the public performance of a play', amongst other types of speech which fall within the remit of this provision, risks a fine of KES.1 million (USD9,258) or imprisonment of 3 years, or both, if found guilty.

As outlined below, this definition does not align with the various interpretations of the right to freedom of expression under Articles 19 and 20 of the ICCPR and risks stifling legitimate expression in Kenya.[6] Furthermore, the UN Human Rights Committee confirmed that the right to freedom of expression extends to expressing opinions, information, and ideas that are 'deeply offensive' and those which 'offend, shock or disturb,' provided these do not constitute an incitement to hatred.[7] Based on this, the imposition of criminal sanctions on abusive or threatening speech that does not constitute an incitement to hatred does not meet the permissible limitations threshold under international law.

[4] Under Article 33 (2) (d), advocacy of hatred includes advocacy that 'constitutes ethnic incitement, vilification of others or incitement to cause harm or is based on any ground of discrimination specified or contemplated in Article 27 (4).'
[5] UN General Assembly, 'Promotion and protection of the right to freedom of opinion and expression, David Kaye (2019) para 17 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/308/13/PDF/N1930813.pdf?OpenElement> accessed 21 April 2021.
[6] ARTICLE 19,' Commentary on the Regulation of 'Hate Speech' in Kenya' (2010) 17-18 <https://www.Article19.org/data/files/pdfs/analysis/kenya-commentary-on-the-regulation-of-hate-speech-.pdf> accessed 25 March 2021.
[7] UNHRC, 'General Comment No. 34' (n 117) para 11; ARTICLE 19, 'Commentary on The Regulation of "Hate Speech" in Kenya' (n 172) 18; *Handyside v the United Kingdom*, judgment of 7 December 1976, Application No 5493/72; *Giniewski v France*, judgment of 31 January 2006, Application No 64016/00 para 43.

False information and publications: The Computer Misuse and Cybercrimes Act, 2018

The prohibitions on 'false publications and the publication of false information, both online and offline, are set out under Sections 22 and 23 of the *Computer Misuse and Cybercrimes Act* (the CMCA) 2018. These prohibitions attempt to regulate information disorder, including 'fake news' and disinformation, in the digital environment and restrict the freedom of expression in Kenya.

Section 22 of the CMCA 2018 prohibits the intentional publication of data which is 'false, misleading or fictitious' or which 'misinforms with the intent that the data shall be considered or acted upon as authentic, with or without any financial gain.' Under this provision, a convicted person can be fined up to KES.5 million shillings (USD45,851) or face (2) two years imprisonment, or both.

Conversely, Section 23 of the CMCA 2018 prohibits the publication of 'false information,' knowingly, and attracts a fine of KES.5 million shillings (USD45,851) and imprisonment of up to ten (10) years, or both. This provision prohibits:

"

(a) The publication of information that is 'false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence among citizens of the Republic,' or

(b) The publication of information which is likely to discredit the reputation of a person.

"

At the outset, any restrictions attempting to address information disorder, be it mis-, dis- or mal-information, 'de facto, limits the right to freedom of expression.'[8] As noted above, any restrictions on the right to freedom of expression must be aligned with the permissible restrictions under international law and Article 24 of the 2010 Constitution.

These two provisions prohibit the publication of information based on the 'falsity of information,' which is not a legitimate restriction under international human rights law. In a 2017 Joint Declaration by four special international and regional mechanisms on freedom of expression on 'fake news', disinformation and propaganda, it was noted that:

"

> The human right to impart information and ideas is not limited to 'correct' statements, that the right also protects information and ideas that may shock, offend and disturb, and that prohibitions on disinformation may violate international human rights standards, while, at the same time, this does not justify the dissemination of knowingly or recklessly false statements by official or State actors.

"

In effect, both provisions create a legal 'duty of truth' where the State, relying on its monitoring machinery, determines what is and is not objective, reliable and factual information and what is and is not truth. This permits the State to police and sanctions the 'desirable' content that individuals can publish and share on their online platforms, including social media platforms, direct messaging platforms, and messaging platforms, which restricts the free flow of information.

[8] ARTICLE 19, 'Submission to UN Special Rapporteur on freedom of expression and 'disinformation'' (2021)<https://www.Article19.org/resources/submission-special-rapporteur-on-freedom-of-expression-and-disinformation/> accessed 25 March 2021.

This control of information also criminalises the intentional sharing of 'false information' which 'serves a social purpose',[9] including the publication of parodies and other forms of literary, artistic and creative expression which critically 'question our lives, perceptions of ourselves and others, world visions, power relations, human nature and taboos,' amongst others.[10] In 2013, the UN Special Rapporteur recalled that any 'expression of political dissent and participation in public debate, including in the form of art, is protected under Article 19 of ICCPR.'[11]

Further, Section 23 of the CMCA re-introduces criminal defamation in Kenya, which was declared unconstitutional in the 2017 *Jacqueline Okuta* case.[12] In 2002, the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression stated that:

"

> Criminal defamation is not a justifiable restriction on freedom of expression and called for the abolition of all criminal defamation laws, and their replacement, where necessary, with appropriate civil defamation laws.[13]

"

Civil Defamation: The Defamation Act

The right to freedom of expression is limited by the *Defamation Act* (CAP 36), which facilitates protecting individuals' reputations, including private and public figures in Kenya. The Act's long title states that the law seeks to 'consolidate and amend the Statute law relating to libel, other than criminal libel, slander and other malicious falsehoods.'

This law gives further effect to Article 33(3), 2010 Constitution, which calls for the 'respect of others' reputation.' This constitutional provision recognises that an appropriate balance must be struck between the right to freedom of expression, the public interest regarding information, and ensuring that no injury is caused to people's dignity and reputation during the exercise of this right.

Kenya's *Defamation Act* disproportionately balances these two rights by failing to protect against vexatious litigation, otherwise referred to as 'Strategic Lawsuits Against Public Participation' (SLAPP), and failing to distinguish between the defamation of public figures, who are expected to tolerate a greater degree of criticism compared to the injury caused to a private individual's reputation.[14] Further, the award of pecuniary damages under Section 16A of the *Defamation Act* is left to judges' discretion, without an attendant requirement to assess the financial capacity of the alleged defamer.[15] Additionally, the *Defamation Act* does not provide a guiding 'maximum award' ceiling for non-material harm.

---

[9] Ibid.
[10] UNHRC, 'Report of the Special Rapporteur in the Field of Cultural Rights, Farida Shaheed' (14 March 2013) UN Doc A/HRC/23/34.
[11] Ibid.
[12] *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR.
[13] 'International Mechanisms for Promoting Freedom of Expression, Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression' (*OAS*, 2002) <http://www.oas.org/en/iachr/expression/showArticle.asp?artID=87&lID=1> accessed 25 March 2021.
[14] Principle 21, Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) <African Commission on Human and Peoples' Rights Presspublic (achpr.org) accessed 27 April 2021.
[15] ARTICLE 19, 'Defining Defamation: Principles on Freedom of Expression and Protection of Reputation' (2017), Principle 19 (b) <https://www.Article19.org/data/files/medialibrary/38641/Defamation-Principles-(online)-.pdf> accessed 23 March 2021.

It has been observed that the failure to assess a defendant's financial capacity during defamation lawsuits is threatening media sustainability in Kenya and risks stifling journalists' and media organisations' ability to express themselves, both online and offline, legitimately.[16]

- ***Regulating the online environment***

The regulation of the online environment and private companies in Kenya has taken two forms, including attempts to impose liability on intermediaries and regulate online platform providers and users. In these instances, State's monitoring and surveillance machinery and capacities raises concerns about the protection of the rights to freedom of expression online, privacy and data protection.

Platform regulation

In Kenya, the regulation of online platforms is governed by various issue-specific legal frameworks, including communications and anti-terrorism laws. These laws create content-related offences which rely on punitive and disproportionate civil and criminal sanctions, which create a chilling effect and risks discouraging select groups, including bloggers, journalists and online publishers of information, from legitimately expressing themselves on issues of public importance given fears of legal censure.

Kenya's telecommunications sector is generally governed by the Kenya *Information and Communications Act* (KICA) 1998, which has been amended several times since its enactment. While various provisions have a bearing on the regulation of platforms, Section 84D of the KICA 1998 has directly affected individuals' ability to express themselves freely online in Kenya. This provision prohibited the publication, in electronic form, of 'any material which is lascivious or appeals to the prurient interest and its effect is such as to tend to deprave and corrupt persons' and attracted a maximum fine of KES 200 000 (USD1,832.54) or imprisonment of 2 years, or both.

In 2019, this provision was declared unconstitutional by the High Court in the *Cyprian Andama v Director of Public Prosecution & another* case. The Court affirmed that this provision was not a legitimate restriction of the right to freedom of expression. Additionally, the Court notes that this provision offended the legality requirement that a law be both 'clear and unambiguous', which failure had a 'chilling effect' on the right to freedom of expression under the 'fear created by the consequences of a charge under the provision.'[17]

In Kenya, the regulation and monitoring of the online environment is also linked to national security and counter-terrorism efforts. The *Prevention of Terrorism Act* (PTA), 2012 provides for the 'detection and prevention of terrorist activities but contains various broad provisions that interfere with the right to freedom of expression online, impacting journalists, bloggers, and online publishers of information. For example, an amendment to the PTA by the *Security Laws Amendment Act*, 2014, introduced a new provision criminalising the 'publication of offending material' which 'directly or indirectly encourages or induces another person to commit or prepare to commit an act of terrorism.' This provision attracts a maximum imprisonment term of 14 years under Section 30A of the PTA.

Crucially, the UN HRC called on States to ensure that,

[16] Mugambi Kiai, Winfred Gakii & Sigi Mwanzia, 'Defamation liability: Razing media outlets to the ground?' (*The Star*, 2020) <https://www.the-star.co.ke/siasa/2021-04-24-defamation-liability-razing-media-outlets-to-the-ground/> accessed 24 April 2021.
[17] *Cyprian Andama v Director of Public Prosecution & another; Article 19 East Africa (Interested Party)* [2019] eKLR < Petition 214 of 2018 - Kenya Law> accessed 27 April 2021.

"

> measures to combat terrorism and preserve national security are in compliance with their obligations under international law and do not hinder the work and safety of individuals, groups and organs of society engaged in promoting and defending human rights.[18]

"

Problematically, Section 30A of the PTA is not aligned with Kenya's international obligations under Article 19 of the ICCPR, which 'protects information and ideas that may shock, offend and disturb.'[19]

Intermediary liability

The UN Special Rapporteur noted that States are imposing obligations on private companies 'to monitor and rapidly remove user-generated content' in laws which are 'likely to undermine freedom of expression even in democratic societies.'[20] These 'demands for quick, automatic removals risk new forms of prior restraint that already threaten creative endeavours in the context of copyright.'[21]

Instructively, in July 2017, the Communications Authority of Kenya (CAK) and the NCIC released the *Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content via Electronic Communications Networks*.[22] These Guidelines imposed liability on social media service providers to 'pull down accounts used in disseminating undesirable political contents on their platform that have been brought to their attention within 24 hours but failed to subject this account removal process to judicial review and oversight. Further, it was noted that the Guidelines delegated 'prior restraint powers' to various private companies without an attendant right of appeal for the party whose content is restricted.[23]

Aside from these Guidelines, intermediary liability can arise based on common law actions (e.g., contract law or a tortious action). Further, intermediary liability for Internet service providers (ISPs) or platform providers can arise based on 'copyright infringement, digital privacy, defamation, national and public security, hate speech, child protection and intellectual property disputes.'[24]

Prior to the enactment of the *Consumer Protection Act, 2012*, previous iterations of the *Consumer Protection Bill,* 2011 defined an intermediary as:

"

> a person who, in the ordinary course of business and for remuneration or gain, engages in the business of —

[18] UN HRC, 'Resolution adopted by the Human Rights Council 22/6' (12 April 2013) UN Doc A/HRC/RES/22/6.
[19] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda (2017) < OAS :: Special Rapporteurship for Freedom of Expression> accessed 27 April 2021.
[20] UN General Assembly, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye' (2018) < 1805436 (un.org)> para 16 accessed 27 April 2021.
[21] Ibid, para 17.
[22] "The Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content via Electronic Communications Networks' <https://ca.go.ke/wp-content/uploads/2018/02/Guidelines-on-Prevention-of-Dissemination-of-Undesirable-Bulk-and-Premium-Rate-Political-Messages-and-Political-Social-Media-Content-Via-Electronic-Networks-1.pdf> accessed 22 June 2021.
[23] ARTICLE 19, 'Kenya: New Draft Guidelines on dissemination via Electronic Communications Networks should be scrapped' (2017) <Kenya: New Draft Guidelines on dissemination via Electronic Communications Networks should be scrapped - ARTICLE 19> accessed 27 April 2021.
[24] Media Defence, 'Intermediary Liability' <https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-5-trends-in-censorship-by-private-actors/intermediary-liability/> accessed 1 April 2021.

(a) representing another person with respect to the actual or potential supply of any goods or services;

(b) accepting possession of any goods or other property from a person for the purpose of offering the property for sale; or

(c) offering to sell to a consumer, soliciting offers for or selling to a consumer any goods or property that belongs to a third person, or service to be supplied by a third person, but does not include a person whose activities as an intermediary are regulated in terms of any other national legislation.

"

Kenya's draft *Intellectual Property Bill* (IP Bill) 2020 refers to and introduces intermediary liability and monitoring requirements on ISPs, with attendant civil and criminal penalties. Specifically, the IP Bill 2020 introduces a notice-and-takedown system that gives hosting services an incentive to remove content without proper notice or evidence of actual infringement, which will have a chilling effect on freedom of expression.

Additionally, the IP Bill 2020 purports to protect ISPs with protection from liability where they are unaware of 'facts and circumstances unless the infringing nature of the material is apparent.' However, it has been noted that this reliance on 'constructive' rather than 'actual knowledge' provides a conflicting requirement for ISPs to monitor content on their platforms, which risks chilling the right to freedom of expression.[25] At the time of writing, the IP Bill 2020 is still undergoing review.

Network disruptions

Unlike its neighbouring countries, including Tanzania and Uganda, there have been no reported incidents of a state-ordered network disruption (e.g. an Internet shutdown) by the State. While a Kenya ICT Action Network report noted that Kenya does not have any 'legal basis for an Internet shutdown,' various laws can be used by the government to justify a state-ordered network disruption. These include state of emergency provisions in the 2010 Constitution, national security and public order laws (the PTA, the *Preservation of Public Security Act*), and hate speech laws (the NCIC Act).[26]

On 16 April 2021, amendments to the Computer Misuse and Cybercrimes (Amendment) Bill, 2021, were tabled before the National Assembly, Parliament. One of the proposed amendments, under Clause 2 of the Bill, seeks to expand the functions of the National Computer and Cybercrimes Coordination Committee to 'recommend that websites be rendered inaccessible in the Republic of Kenya.' The draft Bill has not yet been considered by Parliament, but if enacted, it will amount to an endorsement of state-sanctioned communications disruptions. Generally, this proposed amendment is not in line with international law, with four international mechanisms promoting freedom of expression noting, in 2011, that,

[25] ARTICLE 19, 'Kenya: Intellectual Property Bill must not water down freedom of expression protections' (2020) <https://www.Article19.org/resources/kenya-intellectual-property-bill/> accessed 1 April 2021.
[26] Kenya ICT Action Network, 'Building trust between the state and citizens: A Policy Brief on Internet shutdowns and elections in Kenya (2017) <https://www.kictanet.or.ke/wp-content/uploads/2017/09/Kenya_Policy_Brief_On_Internet_Shutdowns.pdf> accessed 1 April 2021; Part 4, 'Emergency Measures' Constitution of Kenya < Const2010 (kenyalaw.org)> (2010) accessed 27 April 2021.

> cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds.[27]

In addition, the licensing regime in Kenya permits the CAK to suspend communications services, affecting both licensees from providing services, and subscribers, from accessing and using services. For example, the *Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations*, *2014,* permits the CAK to order a licensee to deactivate (i.e., disable access) or suspend (temporarily disable) access of telecommunications services to a subscriber. However, poor documentation makes it unclear what terms and conditions govern the relationship between the CAK and communications providers and whether these permit the CAK to order providers to effect network disruptions.

Before Kenya's 2017 General Elections, the CAK stated that they would shut down the Internet to 'prevent violence' as a 'worst-case scenario' option.[28] The CAK further noted that they possessed a 'social media monitoring system and [had spent] 400 million Kenya shillings ($3.6m) on a device management system that will help us closely monitor mobile phones and the activities around them.'[29] The CAK has exercised these powers of disruption following its interference with the transmission signals of three private TV stations, including NTV, KTN News, and Citizen TV, in 2018. The High Court ordered the restoration of these signals by CAK.[30]

Additionally, in 2018, the CAK announced its installation of the Device Management System (DMS), contested by Mobile Network Operators (MNOs) and human rights organisations in Kenya.[31] One of the documents sent by the CAK to MNO's revealed that the DMS is expected to facilitate the collection of information on International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), and Mobile Station Integrated Services Digital Network (MSISDN) of mobile cellular end-users. The system will then enable the identification of illegal end-user's terminals, which will be listed on the DMS whitelist.' Here, a 'dedicated link' was expected to be created and maintained between MNO's mobile cellular systems and the DMS located at CA Centre's.[32] The rejection by MNOs of this system was based on concerns that the DMS would permit the State to intercept and record communication and mobile data in breach of users' right to privacy. This matter is ongoing and is currently before the Supreme Court of Kenya.

Based on this, it is clear that the CAK, deriving its mandate and powers from KICA, can interfere with the free flow of information online and access to the Internet and other digital communications platforms, but multiple actors are challenging these interferences to ensure the protection of freedom of expression and informational privacy.

---

[27] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the Internet, < empty sheet (osce.org)> (2011) accessed 16 June 2021.
[28] PC TechMag, Kenya's Communication Authority May 'Block Internet' During Elections <https://pctechmag.com/2017/01/kenyas-communication-authority-may-block-internet-during-elections/> (2017), accessed 1 April 2021.
[29] Ibid.
[30] Mercy Asamba, High Court suspends order to shut down TV stations, <https://www.standardmedia.co.ke/kenya/article/2001268124/high-court-suspends-order-to-shut-down-tv-stations> (2018), accessed 1 April 2021.
[31] *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others* [2018] eKLR <http://kenyalaw.org/caselaw/cases/view/151117/>; *Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others* [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/193383>.
[32] *Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others* [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/193383>

- ***Major Incidents***

The Kenyan judiciary has protected the right to freedom of expression online in numerous seminal cases, which continue to affirm the role played by this right in the democratic nation.

The Penal Code

In February 2017, the High Court of Kenya declared criminal defamation offence unconstitutional for violating the right to freedom of expression in the *Jacqueline Okuta & another v Attorney General & 2 others [2017] eKLR* case. In this particular matter, the accused individuals used Facebook to publish statements that were deemed defamatory under Section 194 of the Penal Code.[33] The Court noted that:

"

> the harmful and undesirable consequences of criminalizing defamation, the chilling possibilities of arrest, detention and two years imprisonment, are manifestly excessive in their effect and unjustifiable in a modern democratic society like ours.

"

Here, the Court affirmed that defamation could be addressed by reference to 'an appropriate and satisfactory alternative civil remedy', noting that 'the offence of criminal defamation constitutes a disproportionate instrument for achieving the intended objective of protecting the reputations, rights and freedoms of other persons.'

In April 2017, Section 132 of the Penal Code was declared unconstitutional for violating the right to freedom of expression in the *Robert Alai v The Attorney General & another* [2017] eKLR case. In this particular matter, Robert Alai was charged with using Twitter to publish content which is 'calculated to bring into contempt or to excite defiance of or disobedience to, the lawful authority of a public officer, who in this case is the President of Kenya. The Court noted that,

"

> it is no longer tenable to use laws that are oppressive to the public for the sole purpose of protecting the dignity of public officers, thereby, violating people's right to freedom of expression.

"

Additionally, the Court affirmed that any law which purports to restrict a constitutionally guaranteed right must be,

"

> reasonable, justifiable and the objective of that limitation is intended to serve the society. The standard required to justify limitation is high enough to discourage any limitation that does not meet a constitutional test. And that limitation to a right is an exception rather than a rule.[34]

"

[33] *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR <http://kenyalaw.org/caselaw/cases/view/130781/>
[34] *Robert Alai v The Hon Attorney General & another* [2017] eKLR <http://kenyalaw.org/caselaw/cases/view/135467/>

In May 2021, Section 66 of the Penal Code was declared unconstitutional for violating the right to freedom of expression in the *Cyprian Andama v Director of Public Prosecutions & 2 Others eKLR* case.[35] In this particular matter, Cyprian Andama was charged with the offence of 'publishing alarming information' on his Twitter handle. The Court appreciated that this offence was enacted before the 2010-Constitution was enacted in Kenya and that it had not been subjected to the scrutiny required by Article 24 of the 2010 Constitution on the permissible limits of the rights. However, in its determination, the Court found Section 66 to be:

"

> excessively broad as it is capable of prohibiting the publishing of false statements as well as opinions honestly believed to be truthful hence limiting the citizens' right under Article 35 to access information. A law that limits constitutional rights without any justification violates the Constitution and ought to be removed from the penal laws.

"

The CMCA, 2018

The CMCA, 2018 continues to be challenged in court, both for its vague and disproportionate content-related offences and on procedural grounds. In May 2018, the Bloggers Association of Kenya (BAKE) filed a constitutional petition challenging 26 provisions, including Sections 22 and 23, CMCA[36] , for threatening the rights to expression, media freedom, and privacy. Despite earlier pronouncements suspending the application of these provisions, in 2020, the High Court declared the Act valid and constitutional in its entirety.[37] The matter is currently before the Court of Appeal.

At the procedural level, the Senate lodged a petition against the National Assembly contesting the CMCA's 2018 enactment for failing to adhere to the procedural and constitutional requirements for adopting laws. The High Court, in October 2020, declared the CMCA, 2018 'unconstitutional, thus null and void,' but suspended its order until July 2021 (9-month suspension) to give both houses an opportunity to regularize the laws.[38]

The ability of the CMCA 2018 to control and stifle free speech online continues to be documented by stakeholders in Kenya. For example, before and during official announcements of the coronavirus pandemic in March 2020, Sections 22 and 23 of CMCA 2018 provisions have been used to intimidate, harass, summon and arrest more than ten digital technology users, including bloggers, journalists, content creators, activists, media personnel, students, and politicians.[39]

Notably, the vague nature of these two content-related provisions continues to grant dangerously wide powers to state agents who are abusing and misusing these provisions without adequate oversight. For example, these provisions are being used by state agents to 'target Internet users whose posts countered the government's official Covid-19 narrative' and who 'created and uploaded online content, including posts and websites, commenting on Kenya's political situation and detailing

---

[35] *Cyprian Andama v Director of Public Prosecutions & 2 others; Article 19 East Africa (Interested Party)* [2021] eKLR < Petition 3 of 2019 - Kenya Law >
[36] *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/191276/>. The 26 provisions being contested include sections 5, 16-17, 22-24, 27-29, 31-41, and 48-53, CMCA 2018.
[37] Ibid.
[38] *Senate of the Republic of Kenya & 4 others v Speaker of the National Assembly & another; Attorney General & 7 others (Interested Parties)* [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/202549/>
[39] ARTICLE 19, Freedom of Expression and the Digital Environment in Eastern Africa Monitoring report <Freedom-of-Expression-and-the-Digital-Environment-in-Eastern-Africa.pdf (article19.org)> (2021) pp. 21, accessed 27 April 2021.

corruption scandals.'[40] In one recent case involving an activist, Mutemi wa Kiama, the Court issued orders barring Kiama from expressing himself on matters relating to COVID-19 loans and ordered that his social media accounts be blocked.[41]

In effect, this targeted assault on online users, and the prior restraint orders being issued against individuals by the courts, could create a chilling effect on the right to freedom of expression online.

- ***The right to freedom of expression online: forward-looking practices***

In 2019, attempts were made to amend the KICA 1998 and to regulate the use of social media platforms under the *Kenya Information and Communication (Amendment) Bill (National Assembly Bill No. 61 of 2019).* This 'Social Media' Bill called for the licensing of social media platforms, the sharing of information by licensed persons, the creation of obligations for social media users, the registration of bloggers, and the development of a code of conduct by the CAK.

The 'Social Media' Bill was rejected by the National Assembly's Departmental Committee on Communication, Information and Innovation (NA Committee) for offending the constitutional rights to free expression, media freedom, privacy, and data protection. The NA Committee, relying on arguments submitted by stakeholders, argued that, for example, the definition of 'blogging' to mean everyone on a social media platform and the attendant requirement for licensing before sharing information offended Articles 33 and 34, 2010 Constitution for being vague and unclear. The NA Committee also noted that the processing of personal information provisions had already been canvassed in the *Data Protection Act*, 2019.[42]

3.3.2. Status of data protection in Kenya

- ***Constitutional Provisions***

The right to informational privacy or data protection and communications privacy is guaranteed under Articles 31 (c) and (d), 2010 Constitution. This provision reads that:

"

Every person has the right to privacy, which includes the right not to have—

- information relating to their family or private affairs unnecessarily required or revealed; or
- the privacy of their communications infringed.

"

- ***Other Laws***

The Data Protection Act, 2019

On 8 November 2019, the *Data Protection Act (DPA) 2019* received presidential assent before commencing 25 November 2019. The *Data Protection Act, 2019* is tasked with giving further effect to this constitutional provision and establishing the Office of the Data Protection Commissioner

[40] ARTICLE 19, 'Freedom of Expression and the Digital Environment in Eastern Africa Monitoring report' (2021) 21 <Freedom-of-Expression-and-the-Digital-Environment-in-Eastern-Africa.pdf (Article19.org)> accessed 27 April 2021.
[41] ARTICLE 19, 'Kenya: Release and cease attacks on Edwin Mutemi wa Kiama' (2021) <Kenya: Release and cease attacks on Edwin Mutemi wa Kiama - ARTICLE 19> accessed 27 April 2021.
[42] The National Assembly: Departmental Committee on Communication, Information and Innovation, Report on the Consideration of the Kenya Information and Communication (Amendment) Bill (N.A Bill No, 16 of 2019) <http://www.parliament.go.ke/sites/default/files/2019-12/Report%20on%20KICA%20%28Amendment%29%20Bill%20%28N.A%20Bill%20No.%2061%20of%202019%29.pdf> (2019) accessed 2 April 2021.

(ODPC); making provision for the regulation of the processing of personal data; providing for the rights of data subjects and obligations of data controllers and processors, and for connected purposes.

Despite the DPA 2019 commencing operation in November 2019, data controllers and processors have collected and processed data without proper oversight. Kenya's first Data Protection Commissioner, Immaculate Kassait, was appointed in November 2020, following her nomination and approval by the National Assembly and the President.[43]

The Office of the Data Commissioner has released various guidance notes and guidelines, including the draft *Guidance Note on Access to Personal Data during COVID-19 Pandemic* (draft guidance note), which was released to the public for comments in January 2021.[44] Similarly, the Taskforce on the development of Data Protection Regulations recently released three regulations, including the *Data Protection (General) Regulations), 2021*, the *Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021* and *the Data Protection (Compliance and Enforcements) Regulations, 2021.*[45]

The Access to Information Act, 2016

Before the enactment of the DPA 2019, the protection of personal information in Kenya was provided for, albeit inadequately, under various sector-specific laws, including the *Kenya Information and Communications (Consumer Protection) Regulations, 2010* (confidentiality provision), *the Consumer Protection Act (2012)*, amongst others.

The *Access to Information Act (ATI Act)* 2016 also inadequately provided for personal data protection, with far-reaching effects for the protection of the right. Notably, under Section 21 of the *Access to Information Act* 2016, the Commission on Administrative Justice (or Office of the Ombudsman) possesses data protection functions, which were neither repealed nor harmonised with the functions of the recently-operationalized Office of the Data Commissioner. Thus, for example, the Office of the Ombudsman can 'develop and facilitate public education awareness and develop programmes on the right to access to information and right to protection of personal data', 'work with public entities to promote the right to access to information and work with other regulatory bodies on promotion and compliance with data protection measures in terms of legislation,' amongst others.

In addition, the ATI Act, 2016 and the DPA, 2019 both promote differing definitions of personal data and information, which introduces uncertainty into the law. Under Section 2 of the DPA, 2019, personal data is defined as 'any information relating to an identified or identifiable natural person.' Conversely, Section 2, ATI Act, 2016 provides a more expansive definition of personal information to mean 'information about an identifiable individual, including, but not limited to—

[43] 'Immaculate Kassait appointed as Kenya's first Data Commissioner' (KBC, 2020) <https://www.kbc.co.ke/immaculate-kassait-appointed-as-kenyas-first-data-commissioner/> accessed 2 April 2021.
[44] Office of the Data Protection Commissioner, '(Draft) Guidance Note on Access to Personal Data during COVID-19 Pandemic' (2021) <https://ict.go.ke/wp-content/uploads/2021/01/Draft-Data-Request-Review-Framework-Jan-2021.pdf> accessed 2 April 2021.
[45] *Data Protection (General) Regulations* (2021) <https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf> accessed 24 April 2021; *Data Protection (Registration of Data Controllers and Data Processors) Regulations* (2021) <https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-Registration-of-data-controllers-and-data-processor-Regulations.pdf> accessed 24 April 2021; *Data Protection (Compliance and Enforcements) Regulations* (2021) <https://www.odpc.go.ke/wp-content/uploads/2021/04/THE-DATA-PROTECTION-COMPLIANCE-AND-ENFORCEMENT-REGULATIONS-2021.pdf> accessed 24 April 2021.

"

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, age, physical, psychological or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol or other particular assigned to the individual;

(d) the fingerprints, blood type, address, telephone or other contact details of the individual;

(e) a person's opinion or views over another person;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) any information given in support or in relation to an award or grant proposed to be given to another person;

(h) contact details of an individual.[46]

"

Biometric Data: Digital IDs and Universal Health Coverage

The collection and processing of biometric data precedes the DPA 2019. For example, Kenya's electoral processes have relied on biometric identifiers. In contrast, reports indicate that 'biometric registration was first introduced to Kenya in 2007' with the collection of this data (e.g., fingerprint and iris scans) feeding into the United Nations High Commissioner for Refugees (UN HCR) 'centralized, integrated biometric databases.'[47] Under Section 2 of the DPA, biometric data is defined as 'personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition.'

Kenya's digital ID system, the National Integrated Identity Management System (NIIMS), is a national population register that relies on biometric data for identification purposes under Rule 6 (a), NIIMS Rules, 2020.[48] NIIMS, under Section 3 of the *Registration of Persons Act* collects a wide array of biometric data, including 'fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, and Deoxyribonucleic Acid in digital form.' According to reports, the biometric data of 'over... 37 million Kenyans' was collected during the mass registration exercise and has been 'cleaned up and matched' in anticipation of the 'mass-production of Huduma cards.'[49]

[46] *Access to Information Act* 2016 s 2 < No. 31 of 2016 (kenyalaw.org) > accessed 27 April 2021.
[47] Karen Weitzberg, 'In Kenya, thousands left in limbo without ID cards' (2020) <https://www.codastory.com/authoritarian-tech/kenya-biometrics-double-registration/>) accessed 13 April 2021; Rawlson King, 'Safaricom considers fingerprint biometrics for SIM registration' (2018) <https://www.biometricupdate.com/201808/safaricom-considers-fingerprint-biometrics-for-sim-registration> accessed on 13 April 2021.
[48] The Registration of Persons (National Integrated Identity Management System) Rules, 2020 (2020) <http://citizenshiprightsafrica.org/wp-content/uploads/2020/10/Kenya-Registration-of-Persons-National-Integrated-Identity-Management-System-Rules-2020.pdf> accessed 13 April 2021.
[49] Frank Hersey, 'Huduma Namba digital ID cards to go into production as 2022 election issues raised' (2020)<https://www.biometricupdate.com/202010/huduma-namba-digital-id-cards-to-go-into-production-as-2022-election-issues-raised> accessed 13 April 2021.

In November 2020, reports emerged that the government had deployed a biometric registration process under the Universal Health Coverage (UHC) scheme.[50] This scheme initially captures the biometric data of 'one million poor Kenyan citizens,', but it is unclear where this sensitive personal data will be stored and the safeguards to protect the storage system.

Data protection and cybercrimes

Generally, the protection of individuals' personal data must go hand-in-hand with protection against cybercrimes. In Kenya, the protection of personal data is primarily governed by the DPA 2019. In contrast, cybercrimes are primarily governed by the CMCA 2018, but these two laws provide complimentary safeguards for protecting personal data against cybercrimes.

Despite this, the inadequacies of the CMCA 2018 to deals with cybersecurity issues as reflected by the issuance of the Cybersecurity Guideline for Payment Service Providers, which the Central Bank of Kenya released in 2020. The CBK notes that these guidelines are intended to 'create a safer and more secure cyberspace that underpins information system security priorities, to promote stability of the Kenyan payment system sub-sector.'

- *Major Incidents*

Questioning the Data Protection Act and the NIIMS: Court Cases

In November 2019, the constitutionality of the DPA 2019 was challenged via a constitutional petition, which was filed by Okiya Omtatah and supported by ARTICLE 19, Eastern Africa. The petition raises both substantive and procedural queries, including the independence of the ODPC, the broad exemptions, amongst others. This matter is still before the High Court.[51]

In February 2019, the NIIMS was challenged by human rights organisations on procedural and substantive grounds. Notably, the petitioners magnified that NIIMS would impact and limit the right to privacy and data protection under Article 31 of the 2010 Constitution of Kenya. Specifically, the petitioners noted that the collection of personal information under the NIIMS is intrusive, excessive, and disproportionate; that children's rights to privacy are violated or threatened by the NIIMS; and queried whether the personal information collected under the NIIMS has sufficient legal and data protection safeguards.

In part, one of the major concerns associated with the NIIMS and its collection of biometric data is the centralised design of the system, which creates vulnerabilities, with centralization creating a single point of failure at the point of data processing and storage. This single point of failure exposes users' personal data to hacking or exploitation by state and non-state actors and raises misuse and function creep concerns.[52]

In January 2020, the High Court ordered the government to enact an 'appropriate and comprehensive regulatory framework' for NIIMS, which complied with the 2010 Constitution.[53] Accordingly, in October 2020, *the Registration of Persons (National Integrated Identity Management System) Rules*, 2020, and the *Data Protection (Civil Registration) Regulations, 2020* were gazetted.

[50] Ayang Macdonald, 'Biometric registration for Kenya's universal health coverage scheme underway' (2020) <https://www.biometricupdate.com/202011/biometric-registration-for-kenyas-universal-health-coverage-scheme-underway> accessed 13 April 2021.
[51] Faith Nyasuguta, 'Court declines to suspend Data Protection Act' (2020) <https://www.the-star.co.ke/news/2019-11-21-court-declines-to-suspend-data-protection-act/> accessed on 13 April 2021.
[52] UN General Assembly, 'Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci' (27 July 2020) UN Doc A/75/147 para. 73.
[53] *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties)* [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/189189/>

The latter regulation applies only to specific civil registration entities and gives further effect to Section 71 of the DPA 2019, which sanctions the Cabinet Secretary for Information, Communication, Technology, Innovation, and Youth Affairs to make Regulations.

In October 2020, the Statute Law establishing NIIMS was one of the 22 laws declared 'unconstitutional thus null and void.'[54] However, this order was suspended, until July 2021, to give the Speakers of both Houses of Parliament time to address the due process (procedural) issues affecting these laws.

3.3.3.Intersection of the right to freedom of expression and data protection

In Kenya, the rights to informational privacy and freedom of expression are not only mutually interdependent and reinforcing, but they also occupy the same level of primacy in Kenya's 2010 Constitution, i.e., no right is more superior to the other. The UN Special Rapporteur noted that an 'undue interference with individuals' privacy could both, directly and indirectly, limit the free development and exchange of ideas.'[55] In 2011, the UN HRC in General Comment No. 34 (2011) on the right to freedom of expression, called on States parties to recall that a 'free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression and the enjoyment of other Covenant rights.'

Notably, the enforcement of data protection laws and the promotion of the right to privacy can 'disproportionately impact the legitimate exercise of freedom of expression[56] and media freedom. This recognition builds on calls by the UN HRC to States Parties to ensure that they 'take account of the extent to which developments in information and communication technologies, such as Internet and mobile-based electronic information dissemination systems, have substantially changed communication practices; around the world.'[57]

Journalistic exemption

The intersection between, and the balancing of, the rights to freedom of expression, media freedom, and data protection, and the prioritisation between the right to privacy vis-a-vis the public interest is best exemplified by the 'journalistic exemption' provision in the DPA 2019. Generally, this provision recognises that the processing of personal data can be exempted for historical, statistical, journalistic, literature and art or scientific research.[58]

Notably, this exemption is not a blanket one. However, data controllers and processors who fall within its scope are exempted from complying with numerous data protection obligations, including the limitation to the retention of personal data under Section 39, (1)(d), DPA 2019. Moreover, unlike other jurisdictions, like the EU General Data Protection Regulation (GDPR), or the UK, this exemption does not apply to other data protection obligations, including compliance with data subjects' rights and automated processing cross-jurisdictional transfer, amongst others. This raises queries about the practicality of the exemption, and its prioritisation of the rights to media freedom and free expression, impacting the activities of the media and journalists.

---

[54] *Senate of the Republic of Kenya & 4 others v Speaker of the National Assembly & another; Attorney General & 7 others (Interested Parties)* [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/202549/>

[55] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (17 April 2013) UN Doc A/HRC/23/40 para 24.

[56] ARTICLE 19, 'The Global Principles on Protection of Freedom of Expression and Privacy' (2017) <http://Article19.shorthand.com/> accessed 17 April 2021.

[57] UNHRC, 'General comment No. 34 (n 117).

[58] *Data Protection Act 2019* s 30(b)(viii) <TheDataProtectionAct__No24of2019.pdf (kenyalaw.org)> accessed 17 April 2021.

It is certain that the Data Commissioner's Office, in conjunction with the Cabinet Secretary, will need to expound on this exemption to ensure that the freedom of expression and data protection are adequately balanced and protected in Kenya.

The right of rectification and erasure

The balance between the rights to data protection, access to information, and freedom of expression is best exemplified by the 'right of rectification and erasure' under Section 40 of the DPA, 2019. In addition, the right to rectification and erasure is integral to the accuracy principle under Section 25 (f) of the DPA, 2019, which obliges data controllers and processors to ensure that personal data is 'accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay.'

This provision empowers data subjects to request data controllers or processors to rectify or erase personal data in their possession without undue delay. The DPA, 2019 is categorical that the right to rectification applies where this data is 'inaccurate, outdated, incomplete or misleading and the right to erasure applies where the personal data is irrelevant, excessive or obtained unlawfully, or where the data controller or processor is no longer authorised to retain this personal data.[59] Under this provision, data controllers who have shared a data subject's personal data for processing purposes are obliged to 'take all reasonable steps to inform third parties about a request for rectification or erasure.'

Despite the fundamental nature of this right, it can be limited where personal data is required for 'purposes of evidence.'[60] Here, data controllers and processors are permitted to 'restrict its processing' rather than rectify or erase this personal data. However, an obligation is placed on data controllers and processors to ensure that they 'inform the data subject within a reasonable time.'

While this provision is largely aligned with international standards, this provision fails to provide a period within which data controllers and processors must comply with requests for rectification or erasure requests. The recently released draft Data Protection Regulations, 2021, attempts to cure this gap by providing that data controllers and processors must comply with a request for rectification within seven (7) days of receiving the request, where they 'satisfied that a rectification is necessary.'[61] On the other hand, data erasure requests must be complied with within fourteen (14) days unless the processing is necessary to exercise the right of freedom of expression and information. However, these draft Regulations have not yet been adopted, making it difficult and almost practically impossible for data subjects to properly exercise this right, consequently impacting individuals' rights to know and access reliable and timely information as provided under Article 35 of the Constitution, 2010.

Encryption and anonymity

The protection of freedom of expression and the rights to privacy and data protection is tied to encryption, which is a fundamental feature enabling online anonymity. In keeping with the traditional association of anonymity with the right to privacy, the right to communications privacy is interpreted as protecting anonymity under Article 31 of the Constitution of Kenya, 2010. However, anonymity is also a fundamental aspect enabling the promotion of the right to freedom of expression. The Special Rapporteur on Freedom of Expression affirms that restrictions on encryption and anonymity

[59] Section 40, Data Protection Act <TheDataProtectionAct__No24of2019.pdf (kenyalaw.org)> (2019) accessed 4 June 2021.
[60] Ibid.
[61] Draft Data Protection Regulations, 2021 <Data-Protection-General-regulations.pdf (odpc.go.ke)> accessed 4 June 2021.

must meet the three-part test of limitations to the right to freedom of expression under international law.[62]

The DPA, 2019, introduces new legal protections for digital anonymity and encryption to promote personal data protection in Kenya. Under Section 2 of the DPA, 2019, the term 'encryption' is defined as 'the process of converting the content of any readable data using technical means into coded form' whereas 'anonymisation' is defined as the 'removal of personal identifiers from personal data so that the data subject is no longer identifiable.'

On encryption, the DPA 2019 imposes obligations on data controllers and processors to secure personal data and implement appropriate technical and organisational security measures, including the 'encryption of personal data.'[63] On anonymization, Section 37 of the DPA, 2019 mandates data controllers or processors to anonymise personal data used for commercial purposes, 'in such a manner as to ensure that the data subject is no longer identifiable.'[64] The requirement for personal data to be anonymized is also featured in the limitation of personal data provided under Section 39 (2), DPA, 2019.

Despite these protections, digital anonymity is watered down by the *Kenya Information and Communications (Registration of SIM-Cards) Regulations* (SIM-Cards Regulations), 2015, and the CMCA, 2018. Generally, mandatory SIM card registration has been criticized for 'eradicat[ing] the anonymity of communications, enable[ing] location-tracking, and simplify[ing] communications surveillance and interception. Facilitating the creation of an extensive database of user information places individuals at risk of being tracked or targeted and having their private information misused.' [65]

Despite the implications of such real-name policies and practices, Regulation 11 of the SIM Cards Regulations states that a 'telecommunications operator shall grant the [Communications Authority of Kenya's] officers access to its systems, premises, facilities, files, records, and other data to enable the Authority to inspect such systems, premises, facilities, files, records, and other data for purposes of ensuring compliance with the Act and these Regulations.'[66]

Under the CMCA, 2018, Sections 52 and 53 impact digital anonymity by enabling the police or an authorised person to collect traffic data in real-time (up to six (6) months) and intercept content data (for up to nine (9) months) respectively. However, despite these two provisions being subjected to judicial oversight, with police officers being required to apply for an order or a warrant, both provisions rely on 'reasonable grounds', rather than 'probable cause,' with the former having a lower evidentiary standard. Additionally, despite mandatory court orders being required before the police can intercept or collect traffic or content data, courts in other jurisdictions have still found such provisions unconstitutional for creating profiles for surveillance purposes.[67] The High Court upheld the constitutionality of these provisions, but the matter is being appealed.

---

[62] UN HRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', Frank La Rue < Human Rights Documents (ohchr.org) > accessed 4 June 2021.
[63] Section 41 (4), Data Protection Act <TheDataProtectionAct__No24of2019.pdf (kenyalaw.org)> (2019) accessed 7 June 2021.
[64] Section 37, Data Protection Act <TheDataProtectionAct__No24of2019.pdf (kenyalaw.org)> (2019) accessed 7 June 2021.
[65] 101: SIM Card Registration" (*Privacy International*2019) <https://privacyinternational.org/explainer/2654/101-sim-card-registration> accessed 7 June 2021.
[66] Regulation 11, Kenya Information and Communications (Registration of SIM-Cards) Regulations (SIM-Cards Regulations), 2015 < Registration-of-SIM--Cards-Regulations-2015-1.pdf>
[67] The Supreme Court of Philippines found the provision permitting the collection of real-time traffic data 'does not enjoy the objective reasonable expectation of privacy, [and that] the existence of enough data may reveal the personal information of its sender or recipient, against which the Section fails to provide sufficient safeguard. The Court viewed the law as 'virtually limitless, enabling law enforcement authorities to engage in 'fishing

3.3.4. Major Highlights

(a) The rights to freedom of expression and data protection are constitutionally guaranteed in Kenya.

(b) A range of colonial-era and post-2010 Constitution laws interfere with the proper enjoyment of the right to freedom of expression, both online and offline, in Kenya. The *Computer Misuse and Cybercrimes Act 2018* is the most problematic law affecting the right to freedom of expression online. Since January 2020, more than ten digital technology users, including bloggers, journalists, content creators, activists, media personnel, students, and politicians, have been intimidated, harassed, summoned or arrested using various provisions.

(c) The Kenyan judiciary has protected the right to freedom of expression online in numerous seminal cases. However, in recent rulings, the protection of this right has been trumped by the protection of State interests, as exemplified in the High Court ruling upholding the validity of the *Computer Misuse and Cybercrimes Act*.

(d) The 'Social Media' Bill was rejected by the National Assembly's Departmental Committee on Communication, Information and Innovation (NA Committee) for offending the constitutional rights to free expression, media freedom, privacy, and data protection.

(e) Kenya has a stand-alone law that gives further effect to the right to information and communications privacy. Despite this, the publications of guidelines, rules, and regulations capable of promoting the proper enforcement of the law are still undergoing review and public consultation.

3.3.5. Conclusion

This report has documented the status of the right to freedom of expression and data protection in Kenya by focusing on proximate laws and policies, assessing major incidents including policy implementation, court cases, violations, providing a few examples of forward-looking practices.

Kenya, by virtue of Articles 2 (4) and (5) of the 2010 Constitution, is bound by the general rules of international law, which form part of the law of Kenya. The Republic of Kenya has acceded to numerous international instruments[68] or co-sponsored numerous resolutions, including the foundational Resolution/20/8 on the applicability of rights both online and offline.[69] Despite this, these general rules under international human rights law and constitutional protections have been watered down in national laws, whose interpretation by state agents is interfering, infringing, and violating the rights to data protection and freedom of expression online.

expedition' choosing whatever specified communication they want.' See: *Disini vs. Secretary of Justice (Cybercrime Law)* <Global Freedom of Expression | Disini v. The Secretary of Justice - Global Freedom of Expression (columbia.edu)>

[68] Kenya acceded to the ICCPR on 23 March 1976. Kenya Stakeholders Coalition, UPR, Annexure 3, List of Kenya's Ratification of International Human Rights Treaties <https://lib.ohchr.org/HRBodies/UPR/Documents/Session8/KE/KSC_UPR_KEN_S08_2010_KenyaStakeholdersCoalitionforUPR_Annex3.pdf#:~:text=LIST%20OF%20KENYA%E2%80%99S%20RATIFICATION%20OF%20INTERNATIONAL%20HUMAN%20RIGHTS,Economic%2C%20Social%20and%20Cultural%20Rights%20%28ICESCR%29.%20Accession%2001.05.1972> (2010) accessed 16 April 2021.

[69] UN HRC, 'Resolution 20/8 on the promotion, protection and enjoyment of human rights on the Internet' (2012) UN Doc A/HRC/RES/20/8.

PART 4

Recommendations

/Specific recommendations to state actors/

- **Botswana**

State actors should:

Ensure that the *Data Protection Act of 2018* is commenced and the constitution of the Information and Data Protection Commission is implemented.

Amend the problematic provisions such as those on alarming publication, hate speech and insulting the president as provided under sections 59(1), 92 and 93 of the *Penal Code,* respectively.

Review laws that unjustifiably limit freedom of expression, such as the *Media Practitioners Act of 2008* and *Cybercrimes and Computer Related Crimes Act of 2018*.

Review the powers of search and seizure by the Directorate of Intelligence Security in terms of Section 22 of the *Intelligence & Security Services Act of 2007* as well as section 27 of the *Cybercrime & Computer Related Crimes Act of 2018* to provide means of redress for violations and limit access to devices and the information stored on them.

Enact rights-respecting laws that address thematic areas such as intermediary liability and platform regulation.

- **Ethiopia**

State actors should:

Enact a rights-respecting and stakeholder-driven draft data protection law and ensure the establishment and operationalisation of a Data Protection Commission or any other independent body.

Ensure the operationalisation of an independent and regulatory oversight mechanism concerning communication interceptions and surveillance.

Respect human rights defenders and opposition political parties' privacy by refraining from confiscating phones and spying on their social media accounts and communication materials.

Initiate a constitutional amendment process to expressly reclaim the courts' inherent power of judicial review from a non-judicial body, i.e. the House of Federation.

Re-draft the *Hate Speech and Disinformation Proclamation No.1185/2020* with precision taking the legality requirement under international human rights law into account. These sections include:

- Article 2(2), which has a vague definition of hate speech; Article 2(3) for its sweeping scope, which may violate the legality requirement of Article 19(3) of the ICCPR; and Art 8(1) for its sweeping and overboard provisions thereby violating the provisions of Article 19 of the ICCPR.
- Article 24(1) of the draft Computer Crime Proclamation 2020, which normalises Internet shutdown and censorship.
- The *Computer Crimes Proclamation No.958/2016*. Such revision must provide clear definitions for vague terms such as 'hatred' by taking inspiration from the Camden Principles on Freedom of Expression and Equality, an authoritative but non-binding principle drafted by experts in the field.
- Article 2116(3) the *Civil Code Proclamation No. 165/1960* to adequately define privacy and provide meaningful compensation for damages.

- **Kenya**

State actors should:

Ensure that the transformative nature of the 2010 Constitution is not watered down by primary and secondary laws.

Conduct a comprehensive review of all problematic laws which infringe on the right to freedom of expression online and data protection. This review must be guided by the three-part test under international human rights law, which requires any restriction on the right to freedom of expression to adhere to the legality, legitimacy, necessity and proportionality requirements.

Ensure that the Communications Authority of Kenya discloses its' social media monitoring system' capacity and demonstrate how its deployment protects the rights to freedom of expression and data protection.

Supervise the development and release of guidelines by the Office of the Data Protection Commissioner on the 'journalistic exemption' provision to ensure that the right to freedom of expression and data protection are appropriately balanced.

Amend the following laws in compliance with international human rights standards:

- Section 84(d) of the *Kenya Information and Communications Act of 1998* as decided by the Court in *Cyprian Andama v Director of Public Prosecution & another.*
- Section 30(A) of the *Prevention of Terrorism Act* (PTA) of 2012 to align Kenya's international obligations under Article 19 of the ICCPR.
- Section 16 (A) of the *Defamation Act* disproportionately balances the pecuniary damage award left to the judges' discretion.
- The problematic provisions of the right to freedom of expression under the *Intellectual Property Bill of 2020*.

• Nigeria

State actors should:

Strengthen the Nigerian courts through more training and independence to uphold existing law.

Uphold the rule of law and be guided by internationally set human rights standards and the Nigerian Constitution.

Withdraw the proposed bills to regulate hate speech and the use of social media to allow for more inclusive and diverse deliberations and leave the courts to determine what constitutes hate speech.

Review laws on blocking of contents and platforms to require the independent oversight of the court and not just at the prerogative of a Minister.

Stop the harassment and unjust prosecution of journalists and abide by the Constitution while complying with its international human rights obligations.

For policymakers and legislators

Amend the following law to comply with international human rights standards:

- Section 24(1)(a) of the *Cybercrimes Act* of 2015 as does not define the use of vague terms like 'inconvenience', 'annoyance', or 'insult', which leaves room for vague interpretation and is being used for censorship and suppression of opinion online.
- The *Lawful Interception of Communications Regulations* so that law enforcement agencies cannot access encrypted communications without judicial review.

- Section 45(2)(f) of the *Cybercrimes Act of 2015* such that there should be a judicial review of law enforcement agencies powers to decode or decrypt encrypted information.

Enact a rights-respecting law for determining intermediary liability.

Enact a comprehensive Data Protection Act and ensure an independent data protection authority.

Include provisions on 'journalistic exceptions' in applicable laws and the draft Data Protection Bill.

/General recommendations to non-state actors/

Civil society should:

Monitor the governments' compliance with the rule of law.

Collaborate with relevant stakeholders on the need to ensure rights-respecting legal reforms. For example, there is a need to build additional capacity within each country's legal, civil society and academic research communities to effectively monitor, map and analyse the existing violations of these rights.

Sensitise the public on their free speech and data rights.

Maximise the use of various legal and advocacy tools such as freedom of information requests, strategic litigation, human rights monitoring mechanisms like the Universal Periodic Review (UPR) and others.

Researchers and philanthropy organisations should:

Carry out more contextually relevant research on the need to protect digital rights.

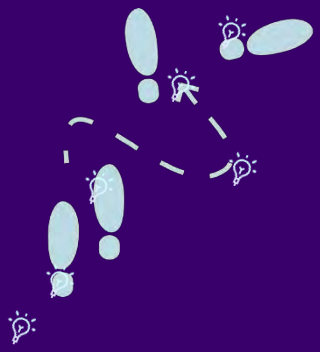
Act as bridges between quality research and policy reform.

Journalists should:

Report more on the various developments concerning the digital rights sector.

Improve their digital safety skills.

Invest in more capacity building to understand the implications of digital rights.



PART 5

General Conclusion

The development of digital rights research, campaigns, and advocacy, especially in Africa, is still growing. In addition to this, the awareness of what they mean is also nascent. Ensuring these, therefore, require concerted efforts towards beaming more focus on these digital rights issues. The primary objective of this report is to examine the two most proximate and affected rights with respect to human rights online–the right to freedom of expression online and the protection of personal information in four African countries, namely Botswana, Ethiopia, Kenya, and Nigeria.

The report finds that all four countries have obligations to protect both rights internationally through their various obligations under the international human rights system and locally through their respective constitutions. This was done by assessing the various incidents that bear on the enjoyment of these rights. Therefore, for each country assessed in this report to comply with their international human rights obligations and constitutions, they must pay close attention to the respective recommendations.

In order to ensure that this is done and carried out effectively, various stakeholders, primarily States, should lead the charge towards amending relevant laws and enacting the long overdue ones. Civil society organisations should also continue to hold States to account concerning these obligations while businesses ensure that their profit-making needs are not the opportunity cost for human rights protection. In ensuring that human rights offline are also protected online, major stakeholders like States, businesses, civil society, the media, research and development, academia and others must commit towards more rights-respecting policies on protecting the right to freedom of expression online and offline.


TECH HIVE
ADVISORY