International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Appraisal of Uganda's Laws and Policies Governing Digital Privacy Protection

**Mr. Hakizimana Janvier[1], Prof. Byaruhanga Archangel Rukooko[2], Dr. Mugwanya Raymond[3]**

[1]PhD candidate, College of Humanities and Social Sciences (CHUSS), Makerere University
[2]Lecturer, College of Humanities and Social Sciences (CHUSS), Makerere University
[3]Lecture, College of Computing and Information Sciences (CoCIS), Makerere University

**Abstract**

This study assesses Uganda's legal regime for protecting privacy in this age of digitalisation. It examines five prominent Ugandan acts that govern digital privacy and their overlaps and contradictions at the local, regional, and international levels. This digital privacy legislation comprises the Uganda National Communications Act 2013, the Computer Misuse Act 2011, the Data Protection and Privacy Act 2019, the National Information Technology Authority-Uganda Act 2009, and the Regulation of Interception of Communication 2010. The study was informed by cybercrimes, digital surveillance, the shutdown of the internet, abuse of rights, and break-ins into offices with a view to target electronic gadgets.

It explores Ugandan government obligations to respect, protect, and fulfil digital privacy in policies, laws, reports, international human rights instruments, and literature. It reveals that some privacy laws are vague, too selective, and seldom applied in practice in Uganda (for example, data protection laws). For instance, the Computer Misuse Act and the Regulation of Interception of Communications Act give state agencies power to spy and eavesdrop on people with minimal transparency, accountability, and judicial oversight. The Data Protection and Privacy Act provides a better balance in data protection and data privacy, but it fails to address digital privacy. It also does not provide tools for encryption and anonymity.

Uganda does not comprehensively protect digital privacy through existing laws. The study finds that existing laws are compulsory and safeguard public interests and national security at the expense of digital rights holders, civil society organisations and individuals. The Ugandan laws promote the unchecked infringement of digital privacy by state security services. In this respect, the study recommends enacting digital privacy legislation consistent with international human rights law, reviewing repressive laws, and supporting independent enforcement agencies to ensure transparency and accountability of digital privacy in Uganda.

## 1.0. Introduction to the scoping review

This chapter examines cybersecurity and privacy laws in Uganda. It highlights regional and international human rights instruments and critiques the five laws governing digital privacy and security in Uganda: the Computer Misuse Act, the Regulation of Interception of Communications Act, the National Information Technology Authority Act, the Uganda Communications Act, and the Data Protection and Privacy Act. It concludes by assessing how the Government of Uganda upholds tripartite (Respect, Protect and Fulfil) human rights obligations in line with digital privacy protection.

### 1.1. Background of the Study

Article 12 of the 1948 Universal Declaration of Human Rights (UDHR) and Article 17(1) of the 1966 International Covenant on Civil and Political Rights (ICCPR) affirm that all individuals possess the right to privacy. However, the 1981 African Charter on Human and Peoples' Rights (ACHPR) omits the right to privacy. The 1995 Ugandan Constitution recognises the right to privacy in Article 27. Privacy has evolved into digital privacy, giving individuals control over how their personal data is collected, stored, used, and disclosed (Chugh, 2023; Singla, 2024). While the UDHR, the ICCPR, and the Constitution of Uganda recognise the right to privacy, advances in surveillance technologies make its protection in the digital age challenging. The digital facet of privacy is largely absent from most international human rights treaties and sustainable development frameworks (Micheal Yilma, 2017). Following Snowden's revelations and the subsequent targeting of whistleblowers who exposed digital State spying powers, the United Nations is providing guidance on digital privacy protection. However, the domestication of digital privacy laws and policies has mainly protected state interests (Molly K. Land & Jay D. Aronson, 2018). The United Nations' efforts to protect digital privacy are not legally binding. Moreover, the enforcement of the 2019 Data Protection and Privacy Act and its 2021 regulations has not effectively addressed the government of Uganda's surveillance powers (Chander et al., 2021). Uganda's constitution and the Data Protection and Privacy Act are commendable steps towards protecting privacy rights. However, they lack effective oversight mechanisms to handle privacy violations committed by State and non-state actors (Muhangi, 2019). Although Uganda's Constitution and Data Protection and Privacy Act establish a basis for privacy rights (Muhangi, 2019; Alice Namuli Blazevic, 2021), deficiencies persist in data protection, consent requirements, and surveillance oversight (Allahrakha, 2024). Furthermore, regressive ICT laws and policies, such as the Computer Misuse Act, confer significant and sweeping powers to security agencies, infringing upon the digital privacy of human rights groups (Benisar, 2010). Human rights NGOs in Uganda have expressed concerns about their digital privacy, asserting that it is vulnerable to security agencies, which specifically target electronic devices such as desktops and laptops during raids and searches (Privacy International, 2015). Case studies on the digital registration of identity cards and the compulsory ID-card-based registration of Internet cafes and Internet subscribers in Uganda and across Africa show that states exploit gaps in legal and policy frameworks to entrench unlawful digital surveillance, thereby violating digital privacy (CIPESA, 2021). Widespread violations and abuses of digital privacy, freedom of expression, and data protection in Uganda and Kenya stem from gaps in digital privacy laws and policies, as well as the application of retrospective legislation (Freedom House, 2023). The UN General Assembly adopted Resolution 68/167 on the right to privacy in the digital era (Humble, 2021) to reshape the human rights legacy in the digital era. Furthermore, the UN Human Rights Council adopted Resolution 25/177, which expresses concerns about digital privacy violations by states and corporations. Because the resolutions lacked concrete principles on Internet rights governance, academics and digital rights advocates have called for a UN Declaration of Internet Rights to address disjointed legal initiatives (Yilma, 2017). African civil society organisations initiated a pan-African human rights movement to urge African States and the African Union to adopt a legal instrument that protects digital rights and freedoms. In 2014, the African Union followed suit by adopting the African Union Convention on Cybersecurity and Data Protection, aiming to align the laws, policies, and practices of its Member States with global consistency in digital data and privacy protection (AU, 2014). Uganda and other member states of the African Union continue to fall short in establishing mechanisms for the protection of digital privacy and security, despite the adoption of the digital rights policy "African Digital Compact-

Agenda 2063" (AU, 2024) and the Digital Transformation Strategy for Africa (2020-2030), which outlines specific measures for implementing encryption and digital privacy standards (AU, 2022).

### *1.2.* Problem Statement

Digital privacy has been a human rights concern since the introduction of computers and the Internet. Following the exposé of the United States' mass digital surveillance, the UN Human Rights Council has urged States to pass laws protecting digital privacy (Falchetta, 2017). Despite the call of the UN Human Rights Council to adopt laws and policies protecting digital privacy and security, the Government of Uganda has passed laws such as the 2002 Anti-Terrorism Act, the 2010 Regulation of Interception of Communication (RICA) Act, the 2011 Computer Misuse Act, the 2013 Uganda Communications Act and other related laws that may violate people's digital privacy. These laws are used to justify violations of digital privacy by the Uganda Police Force (UPF), the Uganda People's Defense Force (UPDF), the Office of the President (State House), and other intelligence and security agencies (Privacy International, 2015). Although certain nations have enacted extensive data protection legislation, such as Uganda's Data Protection and Privacy Act 2019 (Alice Namuli Blazevic et al., 2021) and Zimbabwe's Cyber and Data Protection Act (Saki, 2024), these laws frequently emphasise cybersecurity at the expense of digital privacy. The detrimental effects of existing cyber laws on digital privacy have motivated Ugandan civil society organisations to use human rights documentation technologies, such as Martus, KoboToolbox, and OpenEvSys, to address State digital surveillance and attacks, driven by concerns that State powers may infringe on digital privacy (Nanfuka, 2021).
20b).

## 1.3 Study Objectives

### 1.3.1 General Objective

Assess the efficacy of relevant existing laws, policies, and Uganda's state human rights obligations in protecting the digital privacy of civil society organisations.

### 1.3.2 Specific Objectives

1. Situate digital privacy protection in national, regional and international human rights instruments.
2. Analyse five of Uganda's laws/policies governing digital privacy protection.
3. Examine the extent to which Uganda uphold its human rights obligations in the protection of digital privacy.
4. Devise recommendations to strengthen digital privacy protection in Uganda in line with international human rights standards.

## 1.4. Justification of the Study

This study was motivated by the increasing number of break-ins targeting the digital data of Ugandan civil society organisations (CSOs) and the legal threats to digital privacy. It is particularly critical because it addresses digital privacy for civil society organisations operating in high-risk environments, such as Uganda. It provides essential guidance on sensitive digital data and privacy protection to ensure the security of human rights activists and beneficiaries, equipping them with practical strategies to mitigate risks in 'privacy-poor and surveillance-rich' environments (Vitak et al., 2018). According to African Defenders (2022), office break-ins are a common occurrence in Uganda. In a petition to the Uganda Police Force (UPF), Ugandan civil society organisations (CSOs) described office break-ins as a long-term, systemic, and worsening pattern of attacks on civil society organisations that target their legitimate and valuable work (Monitor, 2017). Although the UPF has not published any investigation reports, CSOs

contend that intruders primarily target digital data because perpetrators of office break-ins target the central processing units of computers, laptops, smartphones, and digital storage devices. CSOs' digital devices were targeted not only by office intruders but also by raids by security agencies. The United States Department of State (2017) reported that, during its cordon-and-search operations, the UPF seized smartphones, laptops, desktops, and digital storage devices belonging to Action Aid Uganda, the Great Lakes Institute for Strategic Studies (GLISS), and Uganda Solidarity (SU). The delayed publication of investigation reports on the break-ins of CSOs' offices and UPF raids motivated this study to examine how Ugandan CSOs protected their digital privacy.

The unchecked legal authority of security services to infringe on individuals' digital privacy and violate human rights served as the second motivation for this study. The digital privacy of civil society organisations (CSOs) in Uganda faces threats, as laws are exploited to abuse and breach human rights (Kibukamusoke, 2022). Countries employ cyber laws to encroach upon their citizens' digital privacy rights. In Uganda, security agencies and other bodies derive such powers through various laws and policies, including the Computer Misuse Act (Rukundo, 2018). This study explored the powers of security services and government agencies as outlined in the Computer Misuse Act (CMA), the Regulations of Interception of Communications Act (RICA), the National Information Technology Authority (NITA) Act, and the Uganda Communications Act (UCA), along with related policies. The Data Protection and Privacy Act (DPPA) and its regulations were also reviewed to assess whether their content and purpose support the safeguarding of digital privacy for Ugandan civil society organisations (CSOs). Not only is Uganda affected by such privacy-invasive laws, but other authoritarian and democratic nations possess similar statutes or practices. All sub-Saharan African countries have passed laws targeting civil CSOs, government critics, and opposition groups (Bussiek, 2022).

## CHAPTER TWO
## REVIEW OF RELATED LITERATURE

### 2.1. The concepts of digital privacy and digital secrecy

As civil society organisations (CSOs) adopt digital tools to protect their online privacy, their operational focus has increasingly shifted to the digital realm. However, confusion between privacy and secrecy has led the Ugandan government to label civil society organisations as secret agents of the West or economic saboteurs for criticising poor governance and the lack of democracy and accountability (Human Rights Watch, 2012). Governments believe that CSOs use secure digital tools because they are involved in illegal activities, such as terrorism (Fowler & Sen, 2010).

Clarifying the distinction between privacy and secrecy establishes a foundation for demonstrating that the use of secure digital technologies aims to ensure confidentiality rather than conceal information that could compromise national security. Privacy and secrecy involve boundaries that restrict access to others. Various scholars and jurists have analysed the scope of privacy. In conceptualising privacy, Solove (2005 ) has summarised privacy under six recurrent themes, namely (1) the right to be let alone; (2) limited access to the self – the ability to shield oneself from unwanted access by others; (3) secrecy – the concealment of some issues from others; (4) control over personal information – the ability to exercise control over information about oneself; (5) personhood – the protection of one's personality, individuality, and dignity; and (6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life. Although many scholars and privacy pundits have adopted such a thematic conceptualisation, point (3) on secrecy has been used by governments to seek legal powers to invade privacy. The US Federal

Court ordered Apple to provide a privacy key of the iPhone to the Federal Bureau of Investigation in a criminal case (The New York Times, 2016).

The secrecy component of privacy has given States in East Africa latitude to enact laws that empower security agencies to infringe on people's digital privacy and acquire digital technologies to invade citizens' privacy (Privacy International, 2015).

The conflation of secrecy and privacy in the digital realm complicates the distinction between these two concepts, necessitating a re-evaluation of privacy. States often view privacy protection tools, such as encryption technologies, not as means of safeguarding privacy but as potential aids for criminals attempting to evade scrutiny by security services (Rider, 2018). This conceptual ambiguity is illustrated by a UK court's decision to order Apple to remove encryption from the iPhone. Human rights organisations, including Amnesty International, argue that the blanket removal of encryption from iPhones poses a global threat to digital privacy (Amnesty International, 2025). They posit that these two terms are distinct, although they are conjoined twins for political interpretations and purposes. Privacy, therefore, refers to the right to control access to personal and institutional information, protecting it from unlawful or unwanted intrusions (Moore, 2007), as well as the obligation not to disclose such information and data to third parties without the consent of the subjects of the data and information (Serohin, 2021). In contrast, secrecy refers to the intentional concealment of information to evade accountability or responsibility (Bruce Wilson, 2024). Maret (2021) expands the description of secrecy by arguing that secrecy in organisations and governments involves intentionally concealing information and data under classified programs to avoid oversight. The secrecy conflicts with the democratic values of transparency and accountability. Government secrecy often covers up covert actions, embarrassments, blunders, and corruption, among other things (Maret, 2011). Individual or organisational secrecy often covers up crimes leading to prosecution (Siegel, 2011). The Ugandan government has recognised that individuals and civil society organisations (CSOs) exposing impropriety, as described above under secrecy, need privacy and protection under the Whistleblowers Protection Act (UPPC, 2010). When CSOs reveal the secrets of individual government officials, they are not secret agents, and they need protection. However, they become secret agents, economic saboteurs, or peace disturbers when they compel unresponsive governments and secretive corporations to reveal their secrets about governance and accountability (Sampson, 2010).

CSOs use established channels, such as whistleblowers and victims, to gather data and information. Therefore, they have the right to both physical and digital privacy and security to protect themselves and to safeguard the privacy of victims, data, information, and their sources (Jagalur et al., 2018).

**2.2. The concepts of digital security and privacy**

Traditionally, security refers to the protection of a state, region, building, or information system. In contrast, privacy is defined as the right to non-interference in one's communications, homes, and correspondence(Tactical Technology Collective, 2014). Digital security and digital privacy are sub-sets of traditional security and privacy in the digital era. Digital security and privacy are embedded in data protection laws and regulations in more than 35 African countries (Hennig, 2018), enabling individuals, organisations, whistleblowers, and activists to share and communicate data securely, beyond the reach of privacy invasions. Digital security and privacy rights are enshrined in international and regional instruments, such as the African Convention on Cybersecurity and Personal Data Protection (Greenleaf & Cottier, 2020).

In the digital era, security and digital privacy are closely intertwined and mutually dependent concepts in data protection. The symbiotic relationship between digital security and privacy necessitates a balanced approach in the digital era, where surveillance is prevalent (Pandey et al., 2024). Digital privacy refers to the ability to control how personal information and data are used. It also refers to the ability of individuals and institutions to decide who has access to their data and information and how these data and information can be used (Idem). Digital security refers to the protection measures implemented to prevent unauthorised access, use, disclosure, disruption, alteration, or destruction of data and information (Tactical Technology Collective, 2014). Digital security and digital privacy are used interchangeably. However, digital security is a means to protect oneself, whereas digital privacy is a result, hence the right. By employing inductive methods, digital privacy experts first identify digital risks and then propose effective digital security measures to protect the right to digital privacy, as illustrated in the table below.

**Table 1: Digital Risk Proofing Strategy**

| | **Digital risks** | **Digital security** | **Privacy** |
|---|---|---|---|
| Definition | Dangers are likely to cause harm | Measures to protect digital data and information | Ability/right to decide prevent unauthorised access, use, disclosure, alteration and destruction of data and information |
| Example 1 | Hacking into email accounts | -Password<br>-Two Factor Authentication (2FA) | The right to prevent email account hacking |
| Example 2 | Interception of email communications | Use secure email browsers such as Gmail. | The right to use secure email browsers. |
| Example 3 | Surveillance | -Use of Tor (The Onion Router) browser-enabled tools<br>-Use Virtual Protocol Network (VPN) | The right to remain anonymous online. |
| Example 4 | Loss of data collected in the field through targeted theft of tablets, smartphones and laptops | -Secure data collection tools such as Martus and KoboCollect will be used. | The right to use secure data collection tools to protect the privacy of organisational data and information. |
| Example 5 | Discovery of secure tools on the smartphones of human rights monitors. | -Use of camouflage and encryption-enabled tools, such as the Tella App.<br>-Use of Vault to hide sensitive phones and audiovisual evidence. | The right to protect data and information from prying eyes. |

***Source: Self-generated by the Researcher (2025), Adapted from DefendDefenders (2024)***

The table above illustrates how digital risks, including digital surveillance and hacking, pose significant threats to the privacy of civil society organisations (CSOs) and beneficiaries. CSOs adopt digital security protocols to protect themselves from prying eyes and ensure they can enjoy the right to privacy as enshrined in international, regional, and national human rights instruments. Governments and corporations have increased their ability to monitor online activities, which necessitates tools to protect user privacy and prevent unauthorised intrusion. The use of secure human rights technologies, such as KoboCollect and Martus services, alongside Virtual Private Networks (VPNs) and anonymous browsers like Tor, enables users to conceal their digital footprints, thereby reducing the likelihood of being tracked, monitored, and blocked (Molly Land, Patrick Meier & Jacob, 2012). CIPESA (2018) notes that past and current reports on governments in Uganda and Tanzania have prompted civil society organisations to utilise encryption-enabled tools, such as Martus, Mailvelope, and Signal Private Messenger, to protect themselves from digital attacks (CIPESA, 2018).

**2.3. Digital privacy protection in international human rights law**

Digital privacy protection is based on the privacy principles guaranteed by human rights treaties. Article 12 of the Universal Declaration of Human Rights guarantees individuals the right to privacy, protecting them from any unauthorised or illegal intrusion into their personal lives, families, residences, or communications (Cristo et al., 2020). The United Nations further emphasised this principle in Article 17(1) of the International Covenant on Civil and Political Rights (1966), reiterating that everyone is entitled to legal protection against unlawful interference or attacks on their privacy (Seibert-Fohr, 2018). Specifically, the right to privacy is of utmost significance for children, as stated in Article 16 of the United Nations Convention on the Rights of the Child (Whalen, 2022). However, it has been noted that the 1981 African Charter of Human and Peoples' Rights (ACHPR) does not include the concept of privacy. The African Commission on Human and Peoples' Rights posits that the incorporation of the right to privacy in the African Charter represents the least burdensome and most expedient approach, effectively reducing the necessity for amendments to articles 66 or 68 of the Charter referring the rights enshrined in the international human rights law (Singh & Power, 2022).

The African Charter's adoption of the right to privacy can mark an important milestone in protecting personal freedoms throughout the continent. Africa has the potential to strengthen its privacy frameworks by examining its challenges and opportunities and learning from best practices in the European Union and the United States. The East African Community (EAC) lacks comprehensive data and privacy protection regulations (Mohamed et al., 2023). This scenario reflects broader dynamics across the African continent, as reflected in the African Charter on Human and Peoples' Rights. Although the AU and EAC charters lack privacy clauses, member States such as Uganda have drawn on international human rights law to embed the right to privacy in their constitutions and legal frameworks. However, the African Commission on Human and Peoples' Rights has noted that the digital communication surveillance laws in Uganda, South Africa, and Nigeria fall short of international human rights standards (Ilori, 2021).

The right to privacy is included in international and national legislation, such as the Universal Declaration of Human Rights (UDHR) and the 1995 Constitution of Uganda. However, these laws do not explicitly address the issue of digital privacy. The strength, capacity, and speed of information and communications technology (ICT) outpace physical privacy protection mechanisms, exposing people to digital privacy invasions. As a result, the lenses through which privacy is defined and protected have shifted due to the digital era. In response to the challenges to digital privacy, the United Nations established a Special Rapporteur in 2011 to monitor and report on emerging issues affecting the enjoyment of digital rights

(Rotenberg, 2017). The Special Rapporteur's reports have highlighted persistent digital privacy issues posed by state and non-state actors, corporate data exploitation, and insufficient transparency in data collection methods (Humble, 2021). They have recommended, among other measures, the establishment of digital privacy legislation, the promotion of digital privacy education, and the availment of technologies that provide digital privacy while considering socioeconomic disparities (Epstein & Quinn, 2020). Under the auspices of the UN, the Internet Rights & Principles Coalition was established and, in 2013, developed a 21-article Charter for Human Rights and Principles for the Internet (CHRPI). According to the CHRPI, States are obligated to protect their citizens' digital privacy, respect the right to use encryption technologies and promote digital literacy education (Van Daalen, 2023). In addition, Article 11(f) of the CHRPI mandates that all individuals have the right to use free and open-source software technologies, such as KoboToolbox and Kobo Collect, to ensure the confidentiality and security of digital data (Internet Rights & Principles Coalition, 2013).

Civil society organisations have echoed a similar call to African States to enact laws protecting digital and data privacy. They issued a declaration akin to the Charter for Human Rights and Principles for the Internet (CHRPI), as seen in the African Declaration on Internet Rights and Freedoms (2014), to guide the enjoyment of digital privacy along with other Internet rights and freedoms. This guidance has yielded notable results, with the African Union adopting conventions and resolutions on digital rights and freedoms, including the 2020 AU Transformation Strategy (ICNL, 2024). The 2020 AU Transformation Strategy marks a significant milestone in digital privacy and data protection, urging African governments to develop and implement robust encryption to protect individuals' digital privacy and security (African Union, 2020). Many African States, including Uganda, have incorporated general data protection and privacy standards into their laws; however, they still lag behind recent international digital rights standards, particularly in encryption (Greenleaf & Cottier, 2018).

### 2.3. Situating digital privacy in Ugandan laws and policies

The government of Uganda has taken positive steps to establish laws regarding digital privacy and protection. However, the enforcement of digital privacy laws and policies often targets political opponents and human rights groups in the name of national security and public interest (Matsiko & Kersting, 2023; Privacy International, 2015). The 1995 Ugandan Constitution and the Data Protection and Privacy Act 2019 affirm the government's commitment to protecting digital privacy and data at rest. However, they do not grant Ugandans the right to use digital privacy technologies, such as encryption tools (Idem). Despite the enactment of the Data Protection and Privacy Act 2019, it remains a paper-tiger law when it comes to enforcement and adequate digital privacy protection (Blazevic et al., 2021). Leveraging its legal arsenal and cooperating with China and Israel to enhance its digital espionage capabilities, the Ugandan government continues to violate the digital privacy of its citizens in the name of national security and public interest (Nanfuka, 2021; Woodhams, 2020). Similarly, several laws, such as the Computer Misuse Act 2011 and the Anti-Pornographic Act 2014, have been enacted to empower security organs to violate and abuse the right to digital privacy and other digital rights (Kakungulu-Mayambala & Rukundo, 2019). Monteleone (2013) posits that digital privacy is a paradox. The disregard for digital privacy can be attributed to the insufficient implementation of practical tools, such as privacy policies and privacy-proofing technologies, both legally and technically. The discrepancy between current digital privacy laws and their implementation in Uganda is willful, as the Government of Uganda and development partners have the technical capabilities to securely customise digital privacy-proofing tools to document and report

data in their various projects. The Uganda development partners, such as the World Bank and the African Development Bank, utilise KoboToolbox and the Kobo Collector Geo-Enabling initiative for Monitoring and Supervision-GEMS (a software based on KoboToolbox) to monitor and supervise most of their projects implemented in Uganda (Morgan, 2011; World Bank, 2019). In addition to financial and technical assistance, the Government of Uganda and its development partners expand the capabilities of project partners in utilising KoboToolbox and KoboCollect GEMS for data collection, privacy improvement, and real-time reporting and visualisation (World Bank, 2019). Civil society organisations are forgotten in these initiatives. In the implementation of Sustainable Development Goals (SDGs), government Ministries, Departments, and Agencies (MDAs) are supported technically in utilising encryption-enabled digital technologies in their operations. The Ministry of Health has developed a robust and secure digital system, the District Health Information System 2 (DHIS2), to securely document and report health data (Ministry of Health, 2021; Wamema et al., 2023). The Uganda Bureau of Statistics (UBOS) has been supported in using a licensed data collection tool, IdSurvey, similar to KoboToolbox and Kobo Collect (Claudia Mancini, 2024), to conduct surveys and the 2024 census (Uganda Bureau of Statistics, 2024a).

Instead of leveraging its expertise in encryption-enabled technologies, such as DHIS2 and IdSurvey, to empower civil society organisations to protect their digital privacy, the Government of Uganda weaponises the laws to suppress digital rights and privacy (Nassanga & Makara, 2016; CIPESA, 2024). Governments in the Global South, including those in Uganda, are interested in practices and laws that ease digital privacy invasion and surveillance (Ahmed et al., 2017).

### 2.3.1. Data Protection and Privacy Act and Computer Misuse Act

Critics have argued that the Uganda Data Protection and Privacy Act 2019 is not sufficiently comprehensive to protect personal data effectively in the digital age (Muhangi, 2019). The Act also faces implementation challenges, including a shortage of resources for monitoring and inspection by regulatory bodies (Bwire, 2023). Despite the Act providing a positive framework for data protection, several challenges persist. According to Van der Merwe (2014), the need for a more robust legal framework is becoming increasingly apparent as the value of digital information continues to rise and it becomes more susceptible to attacks. Digital privacy protection is a mixed blessing that fails to serve as a neutral guarantor and overseer of digital privacy, as demonstrated in the Snowden versus USA case (Van der Merwe, 2014). Despite the Data Protection and Privacy Regulations 2020 being intended to put the Act into force, doubts remain regarding the effectiveness of the legislation (Blazevic et al., 2021). It is possible that future enhancements to the data protection regime could be informed by lessons learnt from industrialised nations and regional initiatives to include the right to use encryption to ward off digital privacy invasion (Greenleaf, 2014).

The 2011 Computer Misuse Act provides severe penalties for unauthorised access to programmes and data, modification of commercial material, and unauthorised use or interception of computer services, among others. According to Kakungulu-Mayambala and Rukundo (2019), the Computer Misuse Act 2011, as amended in 2021, is punitive and intimidating, thereby infringing on the public's freedom to use computers. This Act prohibits the use of any electronic data, book, record, correspondence, register, information, document, or any other material not approved by the government of Uganda. The Computer Misuse Act and other digital privacy laws have been criticised for their potential to suppress Internet freedom, independent journalism and independent human rights documentation and reporting (Selnes, 2021a). Civil society organisations are prone to digital privacy invasions through intrusions or court-

ordered searches. Human rights documenters and reporters are at high risk of digital privacy breaches and require assistance in using digital privacy proofing tools (Notley & Hankey, 2013).

**2.3.2. Electronic Transactions Act and Anti-Pornography Act**

The 2011 Electronic Transactions Act was established to police, secure, facilitate, and regulate electronic data in the form of communications and transactions. While the Internet service provider is not liable for the commissions and omissions of third-party materials in the form of electronic records, it can take down content or a data message if it is informed that the information is unlawful (Tushabe & Baryamureeba, 2007). Furthermore, the Internet service provider does not need a court order to take such action. Civil society organisations (HROs) face a greater risk of digital surveillance and intrusion, even when an individual complains that HROs' information is unlawful. Unwanted Witness (2019) contends that, under this Act, Internet service providers are not obliged to monitor the data they transmit or store, or to seek facts or anything that points to unlawful activity.

The Anti-Pornography Act 2014 criminalises all forms of pornography. The act has faced criticism for its ambiguity, leading to discretionary decisions that may infringe on digital privacy. The Act's provisions concerning the offender registry and the issuance of search warrants without evidence (Nyst & Falchetta, 2017) raise fundamental privacy and data protection issues. A search warrant in court to search premises or computers for pornography does not require evidence of possession of the material, but it also requires evidence that the material is stolen. Digital rights proponents claim that conducting searches without any evidence in order to fight child pornography is a violation of human rights to free people from their control over their lives. The UN Special Rapporteur (Shytov, 2005) has expressed concerns regarding searches, as stated by states that "are only allowed to prohibit child pornography, which is also required by International Law" (Kibukamusoke, 2022). The digital privacy of individuals and civil society organisations dealing with sexual minority issues is particularly vulnerable to surveillance and data breaches (Zalnieriute, 2019). Security services are allowed to seize digital files, computers, phones, or any device containing pornographic material under this Act. Authorities can also search computers, emails, and other electronic devices.

Civil society organisations (HROs) that utilise secure digital privacy tools such as encryption may face legal actions for obstructing access to data requested by the Government of Uganda (Kibukamusoke, 2022), as most governments cite security concerns and cultural decency to justify restrictions on encryption technologies.

**2.3.3. Anti-Terrorism Act and NITA- Uganda Act**

The Anti-Terrorism Act 2002 polices terrorist activities, perceived or real. Enacted in the context of global counterterrorism initiatives following the 9/11 attacks, this Act has faced criticism for its impact on civil society organisations and civil society (Tumushabe, 2015). It has been used to target civil society organisations (HROs) who are perceived to be aiding or working with opposition politicians that the State sometimes views as terrorists or associated with terrorists. Digital privacy concerns have been expressed when States have used anti-terrorism laws to collect metadata and conduct digital surveillance on civil society organisations (Kakungulu-Mayambala & Rukundo, 2019a). Security services have the authority to breach the privacy of digital civil society organisations (HROs) through communication interception and surveillance, as granted by the Anti-Terrorism Act of 2002, as revised in 2017 (Part VII).

The 2009 National Information Technology Authority-Uganda Act (NITA-U Act) has been used to target Civil society organisations (HROs). It grants the National Information Technology Authority Uganda (NITA-U) the authority to monitor internet use in Uganda by both the public and private individuals and

entities. This Act also allows NITA-U to set standards for public hardware and software, including installing spyware, filters, or blocking mechanisms for state surveillance and creating a digital data bank. Data collection on Internet users and civil society organisations is an infringement of human rights, including digital privacy rights (Rukundo, 2018). Under this Act, the Government of Uganda can target all persons, organisations, and their funders involved in so-called anti-government activities. The National Information Technology Authority in Uganda has been used to impede the exercise of digital rights and Internet freedoms, reducing digital rights (Nanfuka, 2021).

**2. 3.4. Interception of Communications Act**

Unwanted Witness (2016) ranks the 2010 Interception of Communications Act as the most detrimental legislation to human rights regarding digital privacy. The law grants specific government officials the authority to request a warrant to intercept communications from a designated judge who is involved in matters outlined in the law. These individuals include the Chief of Defense Forces, the Director of External Security Organisation, the Director General of the Internal Security Organisation, the Inspector General of Police, or their representatives (The Republic of Uganda, 2010). The law states that any ground can justify issuing a warrant to intercept communications. Civil society organisations argue that governments have misused interception laws and regulations, relying on hearsay to violate the right to privacy in Africa (Basimanyane, 2022). The Regulation of Interception of Communication Act, along with other laws, has instilled a profound sense of fear among civil society organisations, which feel they are under constant digital surveillance. An arrest could happen at any moment (Selnes, 2021).

The Regulation of Interception of Communication Act grants service providers the power to intercept communications at all times. Section 8 requires service providers to ensure that all relevant equipment can intercept communications (The Republic of Uganda, 2010). The State's installation of surveillance equipment and applications on the digital devices of Internet and computer users threatens human rights, including the right to digital privacy (Idem). The 2010 Interception of Communications Act legalises the invasion of the digital privacy of Civil society organisations (HROs) in the name of national security (Rusinova, 2021). The law compels Internet and computer users to disclose data encryption keys to government authorities if they have reasonable grounds to believe such information is harmful to the national economy and security. Forcibly disclosing a private key to digital data violates digital privacy and data protection. Third-party service providers have become, de facto and de jure, the trusted spies of governments, and their prying powers are overseen by the selectors of these trusted spies, as well as by security service departments (Fox & Soghoian, 2012). Examples of trusted third parties include hotels that offer free Wi-Fi to guests and passersby, email providers, search engines, and telecommunications corporations. The Act leaves HROs at the mercy of the government regarding data protection and digital privacy, which is why they use encryption-enabled tools.

**2.3.5. Uganda Communications Commission Act**

The 2013 Uganda Communications Commission Act regulates all forms of communication in Uganda. It establishes the Uganda Communications Commission (UCC), whose functions include monitoring, supervising, licensing, inspecting, controlling, and regulating communication services in Uganda. It also receives complaints on communication services and investigates and arbitrates them, among other duties. UCC functions have served as a catalyst in the violations of digital rights and freedoms through blanket or targeted surveillance (Basimanyane, 2022; Ilor, 2023). UCC established a social media monitoring centre and an interception and monitoring centre to conduct internet communication surveillance of individuals and organisations, including civil society organisations (Unwanted Witness, 2016). The UCC

ordered all telecommunication companies to shut down the Internet because it realised that civil society organisations (HROs) and individuals were using Virtual Private Network (VPN) and encrypted tools, not invadable by surveillance services, to disseminate information on human rights violations and abuses committed during the 2021 elections (Roberts, 2021).

**2.3.6. State obligations to protect digital privacy**

Events such as the growth of social media and the release of WikiLeaks' documents have highlighted the need for digital privacy (Chesterman, 2013). On 18th December 2013, the UN passed Resolution 68/167 on the right to privacy and surveillance. A year later, the United Nations (UN) High Commissioner for Human Rights, Navi Pillay, released a report on the right. The report led to the adoption of a second resolution, 25/117, on the right to privacy in 2014. The second UN resolution was "in the context of domestic and extraterritorial surveillance, the interception of digital communications, and the collection of personal data." It discusses the illegality of states' powers to pry into the digital privacy of people and institutions (Warren, 2020). The UN documents confirm that unlawful interference with individuals' privacy and digital communications constitutes a human rights violation (The United Nations, 2014).

The United Nations (UN) recognised that member States have been implicated in digital rights violations and they have grappled with the new concept of privacy in the digital age. The UN established the Special Rapporteur on the Right to Privacy, a digital privacy monitoring mechanism, to monitor states' compliance and uphold their obligations to respect, protect, and fulfil the right to privacy in the digital age (Chander, Nyst 2017). The Special Rapporteur on the Rights to Privacy in the digital age is also mandated to identify actions of digital privacy intrusions without compelling justification, review government policies and laws on the interception of digital communications and collection of personal data, assist government in developing best practices to bring global surveillance under the rule of law, articulate private sector responsibilities to respect human rights and to ensure national procedures and laws are consistent with international human rights obligations. The UN Special Rapporteurs on the Right to Privacy in the digital age have found a significant increase in digital privacy violations, particularly in struggling democracies, including Uganda (Manikowski, 2023). In light of the foregoing, the UN Special Rapporteurs on the Right to Privacy in the digital age have urged UN Member States to use a multidisciplinary approach and work with all stakeholders, including civil society organisations, to establish and update laws and policies to protect digital rights effectively and promote and foster human rights information and education, particularly in the area of personal data protection and privacy (The United Nations, 2024).

**2.3.7. Digital privacy at stake in Uganda**

In Uganda, security services have confiscated electronic gadgets, including computers, that contain sensitive information on oil revenue transparency, land, governance, and human rights. Concerning online privacy and freedoms, Uganda security agencies use and misuse laws to violate digital rights. The Uganda Human Rights Commission (UHRC, 2015) states in its annual report that Uganda has not enacted data protection laws or a right to privacy. It contends that Uganda security agencies use the advantages of gaps in the 2010 Regulation of Interception of Communication (RICA) Act, the 2002 Anti-Terrorism Act and the 2014 Anti-Pornography Act and misuse laws such as the 2011 Computer Misuse Act, the 2013 Uganda Communications Act and the 2011 Electronic Transactions Act to surveil, filter and block online and offline communications (UHRC, 2015 and CIPESA, 2014). Some HROs interpret such actions by the state as a political excess and intrusion into their privacy – particularly access to their data.

HROs covering governance, corruption, accountability and sexual orientation and gender identity (SOGI) issues are the most susceptible to surveillance, censorship, and attacks. Surveillance of netizens' activities

has led to arrests of social media activists (Freedom House, 2015). In the run-up to 2016, the Uganda government threatened to block, filter and censor netizens. Temporary shutdowns of Facebook, WhatsApp, and Twitter took place in late 2015, and prolonged social media blocking was imposed during the 2016 presidential election and the swearing-in of President Yoweri Museveni. Informed netizens had to use VPNs and virtual private networks to circumvent such an Internet blockage. As physical surveillance, blockage, and attacks increase, human rights documenters, reporters and archivists have opted to use the Internet. States and non-state actors have also changed tactics and injected more funds into digital investments to outsmart netizens (Freedom House, 2015). Global Information Society Watch (2015) reports that SOGI activists' email accounts and databases have been hacked, and that some photos and videos have been published in Ugandan tabloids.

A concerning issue is that, in some cases, government agencies have pressured telecommunication companies to provide electronic data and printouts of targeted clients' communications. Privacy International (2015) argues that when legally authorised surveillance is impossible, the Ugandan government secretly targets netizens. The rampant cyber-insecurity has compelled some Ugandan documenters, reporters, and archivists to encrypt their electronic data. They also use internet anonymisers and censorship-circumvention tools, such as the TOR Browser and VPNs. To prevent total information loss in the event of targeted theft and the destruction of computers, servers, and other backups in Uganda, human rights HROs have opted to use cloud backups, such as Google Drive and Dropbox, as well as the servers of other partner organisations located overseas. Given mass surveillance and digital privacy violations, civil society organisations are increasingly turning to secure technologies to combat mass surveillance and digital privacy abuses and violations. They have resorted to using anonymous browsers, such as Virtual Private Networks (VPNs), and secure human rights documentation technologies, including KoboToolbox and Kobo Collect (The National Coalition of Human Rights Defenders Uganda, 2022).

## CHAPTER THREE
## RESEARCH METHODOLOGY
### 3.0. Introduction
### 3.1. Survey and Scoping Review Investigation

Several literature reviews and reports (Privacy International, 2019, and CIPESA, 2018) have documented digital privacy violations and abuses against Ugandan civil society organisations (CSOs). However, reports and reviews assessing how effectively laws and policies protect Ugandan CSOs' digital privacy remain scarce. To the researcher's knowledge, no quantitative analysis or scoping review of digital privacy in Uganda exists. The mixed-methods approach aimed to lay the foundations for a scoping review investigating the legal and policy frameworks that protect Ugandan CSOs' digital privacy. The researcher used documentary analysis and in-depth interviews to assess laws and policies relevant to protecting Ugandan CSOs' digital privacy.

The scoping review analysed five laws and policies on digital privacy in Uganda, namely the Computer Misuse Act (CMA), the Regulation of Interception of Communications Act (RCA), the National Information Technology Authority (NITA), the Uganda Communications Act (UCA), and the Data Protection and Privacy Act (DPPA). It synthesised findings on the likelihood of misinterpretation and misapplication of these five laws, alongside evidence of violations and abuses targeting the digital privacy of Ugandan CSOs. It also identified instances of misuse of the legal framework and unchecked powers that affect digital privacy under the guise of national security and public interest. The scoping review

methodology was preferred over other research methods because it enables researchers to obtain a quick overview of the existing literature on the research topic (Lentferink et al., 2017) and to include various types of studies beyond randomised trials (Arksey & O'Malley, 2005).

### 3.2. Identification of Studies and Search Strategy

A highly sensitive search strategy enabled the researcher to identify, screen, and analyse all studies discussing human rights documentation technologies, digital security, and digital privacy. The researcher reviewed articles, books, reports, laws, and policies published between 2003 and 2022. The researcher also reviewed regional and international human rights instruments governing digital privacy. Google Scholar and IEEE Xplore were searched to identify research articles, papers, policies, reports, and human rights instruments containing information on human rights documentation technologies. The primary data source for Objective One comprised non-scholarly documents such as laws and policies on protecting digital privacy in Uganda. These laws and policies are rarely published in scholarly journals and databases. The researcher also used Google and legal compendia to find relevant legal and policy documents related to digital protection legislation. For Objective One, the researcher used academic search engines to identify scholarly papers, reports, and articles on digital privacy in Uganda and other countries. In all three search engines—Google, Google Scholar, and IEEE Xplore-the search string employed a combination of the following terms: “data privacy and security”, “data privacy”, “cyber-laws”, "data protection and privacy”, “state obligations”, “data security”, “digital privacy”, “digital security”, KoboToolbox, KoboCollect, and “human rights documentation technologies”.

### 3.3. Study selection and the criteria of inclusion and exclusion

The studies, reports, laws, books, and policies included in the review met the following six criteria: 1) Full copies of laws and policies, 2) Full research papers, 3) Empirical research (qualitative and quantitative), 4) Clearly explained research methods, 5) Focus on human rights documentation technologies and digital privacy, and 6) Published in English in 2003 or later. Criteria 1-4 were considered to ensure the reporting of original research and high-quality work. Criterion 5 assessed coherence with the thesis topic and ensured that the documents addressed human rights technologies and digital privacy. Criterion 6 was considered to ensure that the documents were in the language the researcher understands.

### 3.4. Quality Assessment

The analysis of the legal and policy framework aimed at safeguarding the digital privacy of human rights organisations found that laws and policies were the primary focus. A detailed review of all relevant sections and subsections of these laws and policies was conducted. Subsequently, an analysis was drafted. The criteria guiding this analysis were based on the content of the laws and policies regarding digital privacy, their application, the awareness of human rights organisations about these laws and regulations, the powers of State security organs to utilise these laws and policies to either protect or infringe on the digital privacy of human rights organisations, the compliance of human rights organisations with legal requirements, and the satisfaction of Ugandan CSOs with the existing legal framework.

## FINDINGS ON UGANDA’S DIGITAL PRIVACY PROTECTION LAWS AND RELATED STATE OBLIGATIONS

### 4.1. Introduction

### 4.1. Digital privacy veiled in implicit reference

The International Covenant on Civil and Political Rights (ICCPR) Committee said that many cybersecurity and anti-terrorism laws have made it lawful for governments to spy on people and search their private

messages online. They have done so by exploiting the ambiguities of the digital age to claim the right to infringe on people's digital privacy and rights in the name of national security and public interest (Seibert-Fohr, 2018). The advent of digital technologies made it clear that people and civil society organisations had the right to privacy and were protected from arbitrary or unlawful interference with their privacy, correspondence, or unlawful attacks on their honour and reputation under Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights (UDHR) (Office of the High Commissioner for Human Rights, 2026).

Scholars and human rights advocates contend that the ICCPR addresses the traditional notion of physical privacy but does not explicitly address emerging issues, such as online surveillance and invasions of digital privacy in the digitalisation era (Milanović, 2014). Similarly, Article 27 of the Uganda Constitution specifically guarantees the right to privacy in the usual ICCPR language. It does not address digital privacy because the UDHR, ICCPR and the Uganda Constitution were adopted before these technologies existed. Thus, Matzner T. (2019) argues that scholars and non-scholars alike confuse the notions of "privacy" and "digital privacy", which muddies scholarly and policy debates. The African Charter on Human and Peoples' Rights (ACHPR) contains no provisions on privacy; as a result, protecting digital privacy in Africa is difficult (Pretoria University- Centre for Human Rights, 2019). The African Union Convention on Cybersecurity and Personal Data Protection addresses these ACHPR loopholes, although ratification has been slow (Bouke et al., 2014). African States have instead enacted cybersecurity laws, such as computer misuse laws and other surveillance laws, that legitimise intrusion into the digital privacy of individuals, groups, and organisations (Schumann, 2026).

**4.2. Computer Misuse Act (2011)**

The Government of Uganda passed the Computer Misuse Act (CMA) in 2011 to address cybercrimes, online abuses and other online misconduct. But the implementation of the CMA 2011 has not realised its good intentions. Like other States, Uganda has weaponised the Computer Misuse Act (CMA) 2011 and other legislation, such as the Anti-Terrorism Act and the Regulation of Interception of Communications Act, to target dissent, curtail digital rights and criminalise cyberspace (Kakungulu-Mayambala & Rukundo, 2019; Wall, 2010).

Human rights advocates and scholars argued that the enforcement of the Computer Misuse Act 2011 (CMA 2011) is selective, and it has done more harm than good by targeting human rights organisations and critics working on sensitive human rights matters. The Government of Uganda uses CMA 2011 and other laws to impose targeted or mass surveillance and internet shutdowns (Basimanyane, 2025). For more than a decade, human rights advocates have challenged Uganda's Computer Misuse Act 2011 and its selective application (Wanyama, 2026). However, the Government of Uganda has reintroduced the annulled sections and clauses through successive amendments to the Computer Misuse Act 2011. The study critiques Sections 24, 25 and 28 of the Computer Misuse Act 2011 and Sections 23, 26 and 12 of the amended Computer Misuse Act 2022, which enable the Government of Uganda to carry out mass surveillance, invade digital privacy and prosecute critics.

**4.2.3. Computer Misuse Act- Sections 24 and 25: Harassment and offensive communication offences**

Sections 24 and 25 of the Computer Misuse Act (2011) have been misinterpreted and misused to target human rights defenders and government critics (Rukundo, 2018). Scholars and human rights advocates argue that most computer misuse laws are outdated, overbroad, and vague, allowing States to punish critics (Network Security, 2020; Westerhorstmann, 2015).

Sections 24 and 25 of the Computer Misuse Act (CMA) 2011 are overbroad and vague, and the Government of Uganda uses them to target human rights activists, civil society organisations and the opposition. Section 24 provides for cyber harassment. Section 25 deals with offensive electronic communications to annoy, or attempt to annoy, the peace, quiet or right to privacy of any person. An offender convicted of peace-disturbing electronic communications will also be fined and imprisoned for one year under section 25 of the Computer Misuse Act 2011. Scholars and legal experts argue that the language in Section 25 of the CMA 2011 that refers to 'peace' and 'disturbances' is ambiguous and prone to misinterpretation, possibly allowing government security services with invasive powers to invade the digital privacy of individuals and civil society organizations in the name of national security and public interest (Basimanyane, 2025). The Section does not clearly define what constitutes a 'disturbance of the peace' or what is legitimate or illegitimate communication that might lead to punishment. This ambiguity is left to security agents to interpret. The judiciary tends to interpret based on their feelings. This is against the principles of fairness and justice in human rights. Human rights organisations and UN bodies argue that this section is being misinterpreted and misapplied and is often used to target government critics, including civil society organisations (Basimanyane, 2022). The prosecution and conviction of Dr Stella Nyanzi under the Computer Misuse Act are seen as human rights violations. Politicians and government officials mainly use the Act to avoid public scrutiny (Columbia University, 2017). Security personnel's arbitrary arrests of people "offending" this law violate the freedom of expression protected under Article 29 of the Constitution of Uganda and international human rights treaties. The Computer Misuse Act (CMA) 2011 has been challenged twice in the Constitutional Court, but neither challenge has been heard on the government of Uganda's interpretation of the CMA. In response to the human rights abuses resulting from its use, the Principal State Attorney of Uganda has given a noncommittal response, saying that just because the law is contested does not prevent the government from charging people under it (Unwanted Witness, 2019). "Courts only have power to strike down laws when they strike down laws," the attorney added. The government uses the Computer Misuse Act and other laws to hack into people's digital accounts, computers, laptops and devices to monitor and suppress offensive communications and data of human rights organizations and activists. These actions threaten digital privacy and rights on the internet. The wording in the Act is vague and can provide the State with an excuse to use it against you if they suspect you of sending or receiving offensive data or communication. Such communications and data are legitimate only as defined and enforced by the state. The Unwanted Witness (2019) notes that "unchecked interpretation and enforcement can lead to serious human rights violations." A number of Ugandan government critics have been arrested; for example, Kakwenza Rukirabashaija was arrested and arbitrarily detained after a series of tweets criticising President Museveni and his son, forcing him to flee Uganda (ARTICLE 19, 2023). In September 2022, authorities illegally detained Teddy Nalubowa for 13 days on charges of "willfully and repeatedly using electronic communication on Facebook and TikTok to disturb the peace, quiet or right to privacy of President Museveni" (Idem).

In 2023, the Constitutional Court of Uganda annulled Section 25 of the Computer Misuse Act (CMA) 2011, but the government of Uganda continues to use CMA Sections 24 and 25 to deal with computer-related offenses in Uganda, making human rights organisations and activists vulnerable to security services' raids to seize any tools containing information deemed offensive (Basimanyane, 2025). Security services use digital hacking tools to gain unauthorised access to confidential information, thereby breaching digital privacy in combination with other laws such as the Uganda Communications Act and the Regulation of Interception of Communications Act 2010 (Kakungulu-Mayambala & Rukundo, 2019).

**4.2.2. Computer Misuse Act 2011- Section 28: Searches and seizures of computer systems**

Scholars and digital rights advocates have called for cybersearching to be embedded carefully to avoid violating digital rights through remote searching and privacy-invasive technologies (Harvey, 2014). Any items seized shall be returned to the owner within 72 hours of seizure unless the authorised officer makes an inter partes application to court to extend this period of retention as provided for in section 28 of the Computer Misuse Act 2011. This procedural mechanism aims to provide oversight and accountability for law enforcement actions but inadvertently exposes persons and constrains their ability to challenge law enforcement decisions (Gerhardus & Nortjé, 2023). In the 2021 elections, Ugandan security forces raided the civil society election information centre at the Hotel Africana under section 28 of the Computer Misuse Act 2011 (CIVICUS, 2021). They took laptops and cell phones, saying human rights groups had been illegally monitoring the vote. Uganda continues to experience widespread illegal interference, which remains a major, ongoing challenge for human rights organisations working on accountability, governance, and the extractive industry (United States Department of State, 2023).

Section 28 of the Computer Misuse Act 2011's accountability measures make human rights organisations' position precarious and unstable. Section 28 aims to fight cybercrime but can be used to target organisations critical of the Ugandan government. In 2017, concerns over digital privacy rights came in the wake of police raids on ActionAid International Uganda and the Greater Lakes Institute for Strategic Studies (GLISS). In the raid, police confiscated a number of computers and other electronic equipment. However, they have not returned them to their owners which raises serious doubts as to the integrity of the process and its adherence to legal norms (National Coalition of Human Rights Defenders Uganda, 2017). The government has provided no explanation for this unduly long delay, which is alarming as a grave violation of the rights of the persons concerned. The law also allows the recovery of all confiscated items, and it is unlawful for an individual to question the lawfulness or propriety of the court's warrant before the search and seizure is executed (Toit & Toit, 2023).

The Computer Misuse Act 2011 provides no transparency for affected persons and entities, or their legal representatives, to inspect seized computers and electronic devices. In the digital era, today, prior independent oversight mechanisms should be employed in searches and seizures to guaranty transparency and to avoid unauthorised access or disclosure of sensitive information on organisations and individuals (Bernardini, 2023). This is particularly problematic in the digital era, when electronic devices are vulnerable to searches and loss along with sensitive data, spyware and reprisals. - The absence of checks and balances on cyber searches poses serious human rights challenges in an era of intrusive privacy and digital snooping.

The Amended Computer Misuse Act (CMA) 2011 has been welcomed as a positive step forward in protecting children in the digital era. But the revised Section 12 of the CMA 2011 threatens civil society actors who record, document, and disseminate human rights data. Again, the CMA 2011 amendment that seeks to regulate social media and hate speech, unsolicited information and malicious content through the introduction of Section 26 is likely to be used to victimise individuals and institutions that oppose the government narrative.

**4.2.3. Computer Misuse Act 2011, as amended in 2022- Section 23: Child rights in the digital era**

Section 23 of the Computer Misuse Act 2011 recognises and affirms children's basic rights to privacy and protection. It allows computers to send information about children where the sender, sharer and transmitter has the consent of the child's parents or guardians or where the law allows. The sharing must be in the child's best interests. Section 23 addresses sharing information about children and the child rights-based

approach, which prioritises the protection and best interests of the minor above all else. Verma and Mishra (2024) correctly note that including provisions to protect children's rights is a progressive step and aligns with current international frameworks, particularly the United Nations Convention on the Rights of the Child. Alignment is crucial to create an environment where children's rights are recognised and considered, allowing them to develop fully and be socially protected. These Computer Misuse Act provisions reflect the Act's commitment to protecting children's rights and the broader acceptance that national policies should align with international human rights standards.

The importance of consent in protecting children from potential digital harm is clear, but poorly designed consent can act as a barrier to advocacy and support. Manipulating consent for political purposes can, in turn, create barriers for advocates and organizations that work to promote children's rights and wellbeing (Heimer & Pettersson, 2023). This can limit the sharing of important information and transparency. If the standards are too strict, it may be impossible to share important information about what is going on with children's welfare. Additionally, politicized consent processes may damage marginalized populations by limiting access to resources and support. Supervisory bodies on data and privacy protection should ensure that mechanisms for obtaining children's consent are designed and implemented to ensure that they do indeed protect children, and allow for strong advocacy of their rights and needs in the digital environment (Verma & Mishra, 2024). There is a need to strike a balance between these interests, so as to establish an environment in which the rights of children can be promoted. Section 23 of the Computer Misuse Act 2011 is the state's recognition and affirmation of the rights of children to privacy and protection. It states that computers can share children's information with the permission of the child's parents or guardians or where the law allows them to do so by the sender, sharer and transmitter. "Sharing must be in the best interest of the child" Section 23 is on sharing of information on children and the child rights-based approach to with the protection and best interests of the child as the first priority. According to Verma and Mishra (2024), "the insertion of provisions for the protection of children's rights is a progressive step and is well in line with the existing international frameworks, particularly the United Nations Convention on the Rights of the Child." It is essential to align to create an environment where children's rights are known and respected, so that children can achieve their full development and social protection. The provisions in the Computer Misuse Act are an example of the duty of the Act to protect children's rights and the wider principle that national policies should comply with international human rights standards.

The intention of consent is to protect children from potential digital harm. Bad consent architecture undermines advocacy and support. In contrast, the political manipulation of consent can be problematic for the advocates and organisations that work to promote children's rights and well-being (Heimer & Pettersson, 2023). This can restrict the sharing of important information and transparency If the criteria are too narrow, they may prevent sharing important information about issues that affect the welfare of children. Furthermore, the politicisation of consent can restrict access to resources and support for marginalised groups. Supervisory authorities on data and privacy protection should ensure that mechanisms for obtaining children's consent are designed and implemented to protect children and enable strong advocacy for their rights and needs in the digital environment (Verma & Mishra, 2024). It is necessary to balance these interests to promote children's rights in a safe environment.

**4.2.4. Computer Misuse Act 2011, as amended in 2022- Section 12: Criminalising unauthorised data capture**

Section 12 of the Computer Misuse Act (amended) 2022 creates an offense of accessing or intercepting a program and data or information of another person without consent, including a recording of their voice

or recording of video. It also comes with tough penalties, including the possibility of jail time for those convicted of the offenses. "The law is a promise for the digital rights of people in an increasingly connected world. It criminalises these acts and strengthens data protection and privacy. However, the provision, which is meant to combat cybercrime and to protect personal data, has raised concerns about its implications for freedom of expression, digital privacy and the ability of human rights defenders (including whistle-blowers and investigative journalists) and their organisations to carry out legitimate activities that may involve the acquisition or dissemination of information. "Caution must be exercised in the implementation of this Section to avoid the inadvertent stifling of legitimate work in the area of human rights and the free flow of information, both of which are essential to a democratic society."

The new amendments to section 12 of the Computer Misuse Act 2022 will likely be used by state security agencies to monitor and violate the privacy of human rights organisations and individual human rights defenders to prevent them from doing investigative human rights work. But critics say the amendments fall short of providing adequate safeguards against potential abuse of power by citizens. One of the main problems with over-surveillance and illegal collection of personal data is the lack of guidance on how surveillance powers should be used. The Computer Misuse Act 2011 (amended 2022) has expanded government surveillance and could limit freedom of expression and discourage civic engagement as more people become aware that the government may be surveilling their communications and online activities (Murray et al., 2023).

These amendments also reveal a worrying tendency toward greater state control over digital spaces. It is encouraging to see amendments to the cyberlaw that close gaps and remove sections or articles that do not align with international human rights standards. However, human rights groups have documented the Ugandan government's clandestine incorporation of sections or articles in the Computer Misuse Act (CMA) 2011 that arbitrarily privilege national security over individual freedom and rights (M. Davis et al., 2019). Rights activists and academics argue that laws like the CMA 2011 institutionalise digital authoritarianism in Uganda by giving security agencies the power to abuse their authority and infringe on the digital privacy rights of rights activists and critics (Ngamita, 2026).

**4.2.5. Computer Misuse Act 2011, as amended in 2022- Sections 26 A, B and C**

One of the challenges for online human rights and digital rights work in Uganda is the relationship between digital rights and government regulation. In January 2023, to the relief of human rights organisations, Uganda's Constitutional Court struck down section 25 of the Uganda Computer Misuse Act 2011. However, this was short-lived: Parliament amended the Computer Misuse Act in September 2022 to add Section 26(A), (B), (C), and (D). Ironically, in Uganda, when one legal vice was removed, it was replaced with another form of social media regulation enforced more strictly (Solomon et al., 2024). The 2022 amendment to the Computer Misuse Act 2011 has led to more censorship, suppression, and invasion of privacy on social media. 26. Hate speech (A) Unsolicited information (B) Malicious information (C) Misuse of social media (D)

Section 26(A) of the Computer Misuse Act 2011 (amended 2022) states that "*any form of communication that is meant to, or has the effect of, degrading, dehumanising, or encouraging violence or hatred against a person or group based on race, religion, gender, or other trait is hate speech*". But Internet rights activists and scholars argue that governments have used this hate speech provision to control communications and suppress dissent (Basu & Sen, 2024). The problem is that, globally, governments haven't balanced free expression on the net correctly. Computer Misuse Act, 2011. 26 (B) Section 2022 states that sending a person unsolicited information without his/her permission is an offence, unless it is

thought to be in the public interest. Some have criticised the double standards and arbitrary enforcement. "Public interest" is subjective and can be abused to censor online free speech (Neupane & Marasini, 2022). Serious malicious digital activity is an offence under section 26(c) of the Computer Misuse Act 2011 (as amended 2022). However, cyber legislation can create tensions between the public interest and an individual's liberties and freedoms.

A caveat is the combination of sections A, B, and C of the Computer Misuse Act 2011 (as amended 2022). Many human rights defenders and academics have been arrested, prosecuted, convicted or tried for sharing data that the government deems sensitive (Amnesty International, 2026). Social media and human rights activists say the cyberlaws are pushing them to the brink and encouraging techno-authoritarianism (Svobodová, 2025). Governments are seeking to muzzle the print, radio and television media (Afar Abbas, Robina Khan & Imran, 2023; CIPESA, 2025).

#### 4.2.6. Computer Misuse Act 2011, as amended in 2022- Section 26 C

In Uganda, the Computer Misuse Act, 2011 was amended in 2022 to address social media issues. The Section 26 provisions of the CMA 2022/2023 amendments were declared null and void, it was not an offense to o publish, circulate or distribute any information under a false or assumed identity and to use privacy-enhancing tools, including virtual private networks (VPNs), censorship circumvention technology, anonymising tools and others.

According to the Act, the use of privacy-preservation technologies to access YouTube, WhatsApp, Facebook, Instagram, Twitter, WeChat, TikTok, Sina Weibo, QQ, Telegram, Snapchat, Kuaishou, Qzone, Reddit, Quora, Skype, Microsoft Teams, LinkedIn, etc. was considered a crime (The Republic of Uganda, 2022; Kambellari, 2017). Scholars and digital rights advocates argue that VPNs and other anonymity tools constitute a lifeline for individuals and human rights groups, allowing them to bypass state censorship, find alternative narratives and protect their identities (Maitland et al., 2012).

Governments have been reported to use computer misuse legislation to suppress dissent (Neupane & Marasini, 2022; Arthur Arnold Wadero, 2022). The inaccessibility of Facebook and its content without a VPN is a clear example of cyberlaw misuse (Freedom House, 2024). The de jure and de facto bans on VPNs and other technologies that enable users to hide their identity under the Computer Misuse (Amendment) Act 2022 exemplify the Government of Uganda's lack of balance between state control, enjoyment of digital rights, and freedom of expression.

### 4.3. Regulation of Interception of Communications Act (2010)

The Regulation of Interception of Communications Act (RICA) was passed on 5th August 2010 in the wake of the terrorist attacks in Kampala in July 2010. RICA 2010 empowers security services to intercept and monitor communications in transit through the postal services, telecommunication companies and other media of communication, including the Internet. Security services can abuse it to justify illegal invasion of privacy, but the legislation was put in place to combat terrorism and organised crime (Basimanyane, 2022; Eyohgndi et al., 2026). Uganda's RICA 2010 is divided into sixteen sections. This study covers Sections 4, 9, 10, 11, 13 and 14. These sections are related to the safeguards for digital privacy and they form the basis to intercepting communications and related rights.

#### 4.3.1. Warrant of communication interception under RICA Section 4

Section 4(2) of the Regulation of Interception of Communications Act (RICA) 2010 states that some of the interceptors of communications include the Chief of Defense Forces (CDF), the Director General of the External Security Organisation (ESO), the Director General of the Internal Security Organisation (ISO)

and the Inspector General of Police (IGP) and their nominees, all high-ranking government officials. Section 4(2) is vague and overbroad because it does not tie nominees to specific government institutions, so it does not establish traceability of communications-interception activities, nor does it provide legal remedies and accountability for violations. Governments in non-democratic states have exploited this loophole to appoint communications interceptors and evade oversight and accountability for illegal surveillance and invasions of privacy (Basimanyane, 2022; Kanathip Thongraweewong, 2014).

The nominees with no affiliation can be anyone or spying companies that have the technologies to block the Internet, to spy on and invade the privacy of government critics, journalists and human rights advocates. Uganda and other democratic and non-democratic states have used NSO's Pegasus to violate the privacy of government critics and human rights defenders who track, record and reveal sensitive human rights cases (International Council on Archives, 2022), using such legal permissions as an excuse. While some governments have acknowledged using NSO's Pegasus to spy on wrongdoers, they have denied targeting government critics and human rights activists (The Guardian, 2024). The tracing of interceptions and the existence of oversight mechanisms indicate the need for institutionalising processes for intercepting communications. To enhance the legitimacy of the Regulation of Interception of Communications Act (RICA) and the accountability of interception activities, section 4(2) should be amended to state that the nominees shall be deputies of the primary authorised interceptors.

Spyware such as Pegasus does not respect international human rights standards (Defenders Protection Initiative, 2025). Clear delegation of power to authorise communications interception would provide a fair basis for traceability and accountability. The Regulation of Interception of Communications Act (RICA) 2010 aims to protect Uganda from terrorist attacks and organised crime. It is also important to ensure that the Act's implementation does not violate fundamental rights, liberties and freedoms and that legal remedies are provided. Among the interceptors of communications are high-ranking government officials, including the Chief of Defense Forces (CDF), the Director General of the External Security Organisation (ESO), the Director General of the Internal Security Organisation (ISO) and the Inspector General of Police (IGP) and their nominees as listed under section 4(2) of the Regulation of Interception of Communications Act (RICA) 2010. Section 4(2) is vague and overbroad because it does not link nominees to specific government institutions, ensure traceability of communications interception activities, or provide legal remedies and accountability for violations. Governments in non-democratic states have exploited this loophole to deploy communications interceptors and evade oversight and accountability for illegal surveillance and privacy intrusions (Basimanyane, 2022; Kanathip Thongraweewong, 2014).

**4.3.2. Sensitive data in the hands of service providers under RICA Section 9**

Scholars and human rights activists argue that the Regulation of Interception of Communications Act 2010 lacks adequate safeguards for freedom of expression and the right to privacy (Nakintu, 2024). Section 9 of the Regulation of Interception of Communications Act (RICA) 2010 requires government authorities, notably the Uganda Communication Commission (UCC) and telecom providers, to collect extensive data on persons and organisations using their services.

10-Section 9 (1) of RICA states that a service provider/telecommunication company shall obtain—(a) the person's full name, residential address, business address, postal address and his or her identity number contained in his or her identity document, if applicable;(b) the case where the person is a business organization, its business name and address and the manner in which it is incorporated or registered;(c) any other information which the telecommunication service provider deems necessary for the purpose of enabling it to comply with this Act (UPPC, 2010a). RICA 10-Section 9(2) provides that

telecommunication service providers shall ensure that existing subscribers register their SIM cards within a period of six months from the date of commencement of the Act, whereas RICA-Section 9(3) provides that telecommunication service providers shall ensure that proper records are kept of the information referred to in subsection and any change in such information (Idem). The Regulation of Interception of Communications Act (RICA) 2010 gives the Government of Uganda and its security services too much power to monitor and intercept electronic communications, telecommunications and postal communications between individuals, groups and organisations (Nakintu, 2024). RICA 2010, Section 9 (1,2,3) allows telecommunications companies to collect data that enable the Government of Uganda and its security organs to reconnoitre on individuals, groups and organisations to prevent terror attacks and other crimes. While putting sensitive data into the hands of other entities with proper oversight and transparency creates a landscape where digital privacy of individuals, groups and organisations is compromised inadvertently or deliberately.

Governments and telecommunications businesses are breached and misused on a regular basis. Since 9th September 2011, Internet and telecommunications companies have been required to release full details and data to governments for reasons of national security, for they are afraid of losing business (Osinowo, 2019). A notable type of digital privacy compromise in Uganda is unsolicited messaging. This is where network operators, content providers and individuals utilise personal data to advertise or do business without obtaining the requisite authorisation from individuals, groups and organisations. The actions of security services are shrouded in secrecy, and as such there are few studies documenting the digital privacy violations and abuses done by the Government of Uganda and its hired spy organisations. But research and investigations demonstrate that the problems in Uganda's mobile money systems, such as theft and other forms of phishing/vishing/smishing, and fraud, are related to the data and credentials telecommunication firms acquire (G. Ali et al., 2020). Telecommunications businesses commodify and exploit the data of individuals, organisations and organisations for economic benefit, while governments utilise this data to target critics, human rights activists, and journalists (Danton, 2026; Losey, 2015).

Most communications interception laws lack adequate privacy safeguards, weak oversight, and limits on impunity, making them constitutionally flawed (Basimanyane, 2022). Section 9 of the Regulation of Interception of Communications Act (RICA) 2010 permits the collection of data and credentials for intelligence purposes; however, it does not address digital privacy and digital rights. RICA 2010 requires reform to incorporate transparent interception methods, accountability and legal recourse, a balance between national security and individual freedoms, liberty and rights, and lawful use of collected and retained data and credentials (Ryan, 2016).

**4.3.3. Disclosure of protected data under RICA Section 10**

Human rights organisations, human rights advocates, and scholars have argued that the Regulation of Interception of Communications Act (RICA) 2010 needs urgent amendment because it lacks sufficient safeguards to protect human rights and the right to digital privacy (Amnesty International, 2010). Section 10 of the RICA 2010 provides that intelligence services may disclose personal information to authorised persons without notifying the persons concerned. 10 (1) Subject to the provisions of this Act, an authorized person may by notice to the person whom he or she believes to have possession of a key to any protected information, impose a disclosure requirement in respect of the protected information where he or she has reasonable grounds for believing that— (a) the person is in possession of a key to any protected information; and (b) it is necessary to impose a disclosure requirement in respect of the protected information— (i) in the interest of national security; or (ii) for the purpose of preventing or detecting an

offense that may result to loss of life or threat to life; or (iii) for the purpose of preventing or detecting an offense of drug trafficking or human trafficking; or (iv) in the interest of the economic well-being of Uganda. As explained above, the Government of Uganda uses the same reasons, national security and public interest, to compel the gatekeepers of protected information and data to surrender the protection keys, and refusal to do so results in prison sentences or penalties (Apio, 2014).

Section 10 RICA 2010 also falls short of international standards on digital rights, as it does not clarify whether or not prior judicial authorisation is required for a person to be able to disclose protected information (Amnesty International, 2010). Section 10 of the Regulation of Interception of Communications Act (RICA) 2010 bears a passing resemblance to the blunt instruments security services use in physical raids and office break-ins. Politics and technology have allowed governments to violate digital privacy without sufficient justification (Inam et al., 2023). Human rights advocates and scholars argue that this section reflects physical raids and office break-ins that have become digital raids and digital office break-ins. Most legislation on communications interception sidesteps the niceties of 'knocking and asking' for entry, since those in possession of protected information are obliged to give up the keys (Cohen, 2000). This Section gives unchecked, sweeping authority to force holders of encryption keys to disclose encrypted data. It violates the constitutional rights guaranteed by Article 27 of the Uganda Constitution 1995, which prohibits unlawful interference with the privacy and correspondence of persons, groups and organisations.

**4.3.4. Provision of interceptable services under RICA Section Eleven**

Section 11 of the Regulation of Interception of Communications Act (RICA) 2010 places individuals, groups, and organisations in a more precarious position than Section 10. Various studies show that interception legislation worldwide has lacunae that shroud State practices in targeted or bulk surveillance and digital ‘bedroom’ privacy in total secrecy(Saki, 2025). The Ugandan Government has exploited the absence of international human rights standards to enact liberticide cyber laws or policies. Section 11 of the Regulation of Interception of Communications Act (RICA) 2010 places individuals, groups, and organisations in a more precarious position than Section 10, as it sets out the ultimate purpose of communications interception in this digital era. It requires the telcom firms and digital service providers to use devices and services that can be intercepted and decrypted. Section 11 of RICA 2010 sets out the detailed conditions telecommunications companies must follow to ensure interception readiness, assist the Government of Uganda in intercepting telephone and online communications, and retain calls and metadata. It reads as follows: “ *(1) Notwithstanding any other law, a telecommunication service provider shall— (a) (b) provide a telecommunication service which has the capability to be intercepted; and store call-related information in accordance with a directive issued under subsection (2). (2) The Minister responsible for Information and Communications Technology shall, on the commencement of this Act, issue a directive to telecommunication service providers specifying— 16Regulation of Interception of Act 18 (a) (b) (c) Communications Act 2010 the manner in which effect is to be given to subsection (1) by every telecommunication service provider; and the security, technical and functional requirements of the facilities and devices to be acquired by every telecommunication service provider to enable— (i) (ii) the interception of communication under this Act; and the storing of call-related information; and the period within which the directive must be complied with. (3) A directive referred to in subsection (2) shall specify— (a) (b) (c) (d) the capacity and technical features of the devices or systems to be used for interception purposes; the connectivity of the devices or systems to be used for interception purposes with the monitoring centre; the manner of routing intercepted information to the monitoring centre; and any*

*other relevant matter which the Minister responsible for Information and Communications Technology deems necessary or expedient. (4) Notwithstanding any other law, agreement or licence, a telecommunication service provider shall, at its own expense, acquire, whether by purchasing or leasing, the facilities and devices specified in a directive issued under subsection (2). (5) Subject to section 12, any cost incurred by a telecommunication service provider under this Act for the purpose of— (a) enabling— 17Regulation of Interception of Act 18 (b) Communications Act (i) (ii) 2010 a telecommunication service to be intercepted; and call-related information to be stored; and complying with this section and section 8; shall be borne by the telecommunication service provider. (6) A directive issued under sub-section (2) may in a like manner be amended or withdrawn*". The above Section and its sub-sections direct digital service providers and telecommunication firms to facilitate the interception of all communications and data in transit or at rest, putting individuals, groups and organisations in danger. Studies confirm that the Government of Uganda uses advanced spying technologies to conduct targeted or bulk surveillance and invade the digital privacy of civil society organisations and critics (International, 2019; Ngamita, 2026). In response to vulnerabilities linked to overt and covert interception of communications and invasions of digital privacy, individuals and civil society organisations have turned to un-decryptable products such as Apple Products (iPhones and Mac laptops) and secure digital tools such as VeraCrypt, KeePass, and KoboToolbox/KoboCollect(Lowell, 2017; Zinkus et al., 2021; and Maneesh & Prodduturi, 2025). Although the Government of Uganda has not outlawed encryption to avoid international backlash, its security services and other ICT agencies continue to use unlawful tactics to conduct targeted or mass surveillance and hack into the encrypted data and communications of individuals, groups, and organisations. Civil society organisations have been targeted through office break-ins, confiscation of digital gadgets, theft of computers/servers and spyware such as Zeus malware and Pegasus (International, 2019). International human rights standards require governments and service providers to protect digital privacy and ensure stringent oversight and transparency in the lawful invasion of the privacy of individuals, groups, and organisations. However, global intelligence practices show that security services disregard privacy safeguards in their daily covert and overt operations, underscoring the need for effective mechanisms to protect digital privacy rights (Finn & Prescott, 2025).

**4.3.5. Retention of postal articles under RICA 2010 -Sections 13, 14 and 15**

Sections 13, 14, and 15 of the Regulation of Interception of Communications Act 2010 (RICA 2010) empower the Government of Uganda to retain and examine postal articles (mail and parcels) and disclose information about them without the recipient's consent or notification.

Section 13 of the Regulation of the Interception of Communications Act 2010 (RICA 2010), which governs the retention of postal articles, does not consider the intended recipient's privacy rights. It stipulates as follows:

*(1) Where an authorised person suspects on reasonable grounds that a postal article in the custody of a postal service provider-*

*(a)contains anything in respect of which an offence or attempted offence is being committed;*

*(b)contains anything that will afford evidence of the commission of an offence;*

*(c)is being sent to further the commission of an offence; or*

*(d)needs to be obtained and examined in the interests of defence, public safety or public order, he or she may apply to a designated judge for a retention order to retain the postal article for the purpose of examination.*

*(2)Where a designated judge, by written order to the authorised person and the postal service provider, certifies that it is necessary for any of the purposes specified in subsection, to order that a postal article in the postal service provider's custody should be retained and, if so required by the order, opened and examined, the postal service provider shall forthwith retain the postal article.*
*(3)Section shall apply with such modifications as may be necessary to the information required to be furnished to a designated judge before a retention order is issued.*

Section 13 of RICA 2010 shows complete disregard for the intended recipient of the retained postal articles, and it is a deal between postal service providers and the government, unbeknownst to the intended recipient. While courts may allow interference with the privacy of the recipient of postal articles (mails and parcels), scholars and human rights advocates argue that the right to privacy is absolute and that the intent of postal articles must be that the recipient is aware of any lawful invasion of their privacy (Gopi C.C., 2026).

The exclusion of the intended recipient of the postal articles (mails and parcels) continues in the subsequent two sections of RICA 2010. Section 14 of RICA 2010 disregards completely the consent of the intended recipient of postal articles as it stipulates that:

"*(1)On the day appointed by or under a retention order, the authorised person shall, in the presence of a representative of the postal service provider, examine the retained postal article.*
*(2)Where, on examination of a postal article under subsection, the suspicion that gave rise to its examination-*
*(a)is substantiated, the postal article may be retained for the purposes of evidence in a criminal prosecution or destroyed or dealt with in such other manner as may be authorised by the retention order;*
*(b)is not substantiated, the postal article shall be delivered to the person to whom it is addressed or to his or her representative on payment of the postage payable on the article.*

The above Section is incompatible with international human rights standards because it allows postal officers or security services to inspect or examine retained postal articles without notifying the intended recipient or obtaining his/her consent. National, regional, and international human rights instruments enshrine the inviolability of postal correspondence(American Journal of International Law, 2017). However, studies show that governments worldwide enact laws and amend existing legislation to legalise total secrecy in inspecting or examining retained postal articles, a practice widespread in both democratic and non-democratic countries (Rooney, 2017).

Section 15 of RICA 2010 drives the final nail into the coffin of total concealment surrounding the invasion of privacy in postal correspondence, complementing Sections 13 and 14. Although it restricts the disclosure of any communication or information relating to postal articles, this Section (in its exception clause) authorises disclosure to agents of the Government of Uganda, as it stipulates that:

*(1)No person may disclose any communication or information which he or she obtained in the exercise of his or her powers or the performance of his or her duties under this Act,* ***except****—*
*(a)to any other person who of necessity requires it for the like exercise or performance of his or her functions under this Act;*
*(b)information which is required to be disclosed under any law or as evidence in any court of law.*
*(2)No—*
*(a)service provider or protected information key holder may disclose any information which it obtained in compliance with this Act;*

*or(b) an employee of a service provider or protected information key holder may disclose any information which he or she obtained in the course of his or her employment and which is connected with the exercise of any power or the performance of any duty under this Act.*
*(3)Any person who discloses any information in contravention of subsection commits an offence and is liable, on conviction, to a fine not exceeding one hundred twenty currency points or to imprisonment for a term not exceeding five years, or both.*
*(4)The Minister responsible for information and communications technology may revoke the licence of any service provider or protected information key holder who discloses any information in contravention of subsection.*

This Section does not protect the privacy of the recipient of postal articles, as there is no single provision addressing the postal article recipient's rights in the communication/information disclosure processes. The drafters of the Regulation of the Interception of Communications Act (RICA) in all countries intentionally legalise violations of the rights of recipients of postal articles (mails and parcels) by omitting specific clauses on privacy rights (Luck, 2014). Under Section 15 of the Regulation of the Interception of Communications Act 2010 (RICA 2010), the Government of Uganda and postal service providers have the prerogative to disclose communications or information in postal correspondence, and the recipient of the postal articles must not be aware of the disclosure and must not consent to such a disclosure.

Sections 13, 14, and 15 of the Ugandan Regulation of the Interception of Communications Act 2010 (RICA 2010) allow agents of the Government of Uganda and postal service providers to retain and inspect/examine postal correspondence and disclose related information or communications in total secrecy. The lack of transparent, independent mechanisms to oversee the retention and examination of postal articles and the disclosure of related information or communications continues to exacerbate the privacy of postal correspondence recipients, leaving aggrieved recipients powerless against overbearing government overreach (Bruce, 2018).

### 4.4. National Information Technology Authority - Uganda Act (2009)

The National Information Technology Authority -Uganda (NITA-U) is a Government agency in Uganda established under the NITA-U Act of 9th July 2009 to coordinate and regulate Information and Communications Technology (ICT) standards in the public and private sectors. The legislation has also identified NITA-U as the lead in the development of data protection and privacy policies and regulations and the development of standards for hardware and software (NITA-U, 2012). NITA-U is the National Data Bank's data breach protection guard. The agencies managing the national data bank should employ robust data protection measures such as encryption tools and easy-to-use means for individuals to report breaches and seek redress (Tolani & Pareek, 2024). NITA-U oversees the rationalisation of IT initiatives across MDAs and the efficient use of technology in the public sector. But it has kept civil society, in particular rights groups, at arm's length. Under Section 32 of the NITA-U Act, NITA-U promotes a healthy digital environment in consultation with human rights organisations.

#### 4.4.1. NITA- Uganda's strides in rationalising government ICT initiatives

NITA-Uganda (NITA-U) has developed and implemented a standard ICT framework to meet the needs of the Government of Uganda Ministries, Departments and Agencies (MDAs). NITA-U has enhanced civil servants' knowledge and skills to support efficient, effective public sector operations by rationalising ICT interventions across government (NITA-U, 2020). NITA-U has provided a framework for integrating ICTs and encouraged agencies to work together rather than in silos.

This section provides a snapshot of the Government of Uganda Ministries, Departments and Agencies (MDAs)' digital initiatives using DHIS2, KoboToolbox, KoboCollect and IdSurvey. In 2011, the Ministry of Health adopted DHIS2 as its digital platform for data collection, analysis and visualisation. The Ministry of Health (MoH) uses DHIS2 to manage 20 Program Implementation Action Plans (PIAPs) and to track the specific results, outputs, activities and resources required to achieve program or indicator targets (DHIS2, 2025) in its Monitoring and Evaluation (M&E) process. The deployment of DHIS2 has facilitated the use of the e-government platform by all Ministries, Departments, and Agencies (MDAs) of the Government of Uganda. Overall, DHIS2 has 11,327 indicators, of which 5,553 are visualizable (DHIS2, 2026). The Ministry of Education and Sports' Basic Education Department has decentralised DHIS2 to district education officers and leadership for data collection, visualisation of data, and data analysis for routine planning, resource allocation, monitoring, supervisory support and evidence-based decision-making (UNESCO, 2020). The digitisation of data documentation by the Ministry of Sports has attracted the attention of a number of partners and funders, including NORAD, GPE KIX, the World Bank, Save the Children and the World Food Programme.

Recently, the Government of Uganda and partners like the United Nations Children's Fund (UNICEF) have collaborated to develop a more user-friendly digital system in schools to gather crucial data such as latrine facilities, available classrooms, and desks for learners, facilitating better planning and implementation (UNICEF, 2024). Teachers with limited computer skills can perform school censuses, teacher monitoring, learning assessments, infrastructure audits, community mobilisation, and geolocation evidence gathering. This is why it is important to introduce KoboToolbox and KoboCollect. KoboToolbox and KoboCollect are free online tools that help non-profits track activity metrics and ensure resources are used according to result indicators (World Bank, 2022). As part of the Uganda Vision 2040, the Uganda Bureau of Statistics has been mandated to digitise censuses using the data documentation tools. The Government of Uganda is using electronic devices such as tablets and laptops in the 2024 National Census to improve data collection and reporting (Uganda Bureau of Statistics, 2025). The Uganda Bureau of Statistics has also used the IDSurvey suite for small-scale surveys and similar tools, as well as for large-scale surveys like the National Population and Housing Census 2024 (Idem). NITA-U's digital initiatives boost public-private partnerships. NITA-U can also tap into the private sector's expertise, resources, and innovative solutions, as well as human rights organisations.

#### 4.1.3. Underutilised window of collaboration between NITA and organisations

Section 32 of the National Information Technology Act (2009) mandates the National Information Technology Authority-Uganda (NITA-U) to coordinate and collaborate with other institutions to develop a conducive technical and regulatory framework for the provision of reliable and secure e-services. The United Nations (International Communication Union, 2025) underlines the importance of collaboration between government and private organisations to improve the availability and accessibility of digital technologies for citizens.

The Government of Uganda Ministries, Departments and Agencies (MDAs) and the civil society organisations are equal partners in the ICT initiatives. As mentioned in the previous section, NITA-U has supported government MDAs to use secure data documentation tools such as DHIS2, KoboToolbox, Kobo Collect and IdSurvey. But it has not helped human rights groups. The NITA-U's apparent reluctance to provide guidance, and its failure to respond to the digital privacy and security requirements of these organisations, raises concerns about its commitment to its statutory duties. This (non) engagement with

civil society on this key issue can be seen as a deliberate disregard for the rights of organisations operating in an increasingly hostile digital environment.

As online laws and regulations become increasingly regressive, human rights organisations in Uganda have partnered with tech experts and organisations to leverage secure documentation tools like Martus, Signal Private Messenger and Mailvelope (CIPESA, 2018). They hoped to use tools, such as encryption, to protect privacy if the Data Protection and Privacy Bill 2015 became law. In response to regressive online laws and regulations, Ugandan human rights organisations have worked with technology experts and organisations to use secure documentation tools such as Martus, Signal Private Messenger and Mailvelope (CIPESA, 2018). The Data Protection and Privacy Bill 2015 was supposed to provide them the ability to use privacy protection tools such as encryption. The year 2018 was a turning point for human rights groups in Uganda, especially regarding digital data and privacy protection, with the retirement of long-term digital archiving technologies (Benetech, 2018). NITA-U's inaction comes as the Data Protection and Privacy Act was assented to law in 2019, which was meant to provide privacy-preserving technologies.

The National Information Technology Authority Uganda (NITA-U) Act was a step forward, but it lacked tools to protect privacy such as encryption (Blazevic et al., 2021). The law has no specific provisions on encryption and other advanced privacy mechanisms, and stakeholders say it does not go far enough to protect human rights organisations' sensitive information. Because of weaknesses in the current legal framework and the expiry of Martus and other human rights documentation technologies, human rights organisations in Uganda are currently forced to use other technologies with better security and privacy. Civil society organisations mostly opt for KoboToolbox and KoboCollect as they are secure and low-cost. KoboToolbox and KoboCollect have empowered human rights organisations to gain greater control over data and to reduce the risk of data breaches and unauthorised access (DefendDefenders & Kobo, 2024). Encryption tools such as KoboToolbox, KoboCollect, Tella App, and Signal Privacy Messenger were also used to encrypt data in transit and at rest and maintain anonymity in politically sensitive working environments (Cheah & Quah, 2021; Dizon et al., 2022).

### 4.5.Uganda Communications Act (2013)

The Uganda Communications Commission (UCC) is the communications sector regulator under the Uganda Communications Act, 2013. The UCC also licenses communications service providers such as radio stations and telecommunication companies to operate. Scholars and digital rights advocates sometimes see the UCC operating arbitrarily to the detriment of digital rights (Walyemera, 2021).

The Uganda Communications Commission (UCC) describes a mission, but studies show that its actions go beyond regulating communications. The UCC also restricts communication by blocking certain Internet users from visiting certain websites and by blocking Internet access nationwide (Solomon et al., 2024). However, studies have shown that the UCC has been used to silence critics of the Government of Uganda, including vocal human rights groups and activists (Nanfuka, 2021). The UCC's interference contravenes the rights to freedom of expression and information provided for under international human rights instruments such as the International Covenant on Civil and Political Rights (Kakungulu-Mayambala & Rukundo, 2019). Governments use communications authorities or similar agencies to shut down the Internet or to stop the flow of sensitive information (Madapathi, 2024).

Research by academics and human rights defenders also revealed the role of the Uganda Communications Commission (UCC) in the social media shutdowns of 2021 and 2026 and a nationwide internet shutdown

to prevent people and civil society organisations from documenting and reporting on human rights violations and abuses in relation to general elections (Amnesty International, n.d.). The UCC's censorship powers have also spurred Ugandan civil society organisations (CSOs) to innovate and build resilience in documenting and reporting human rights abuses and violations, as discussed in the following sub-sections.

**4.6.1.UCC indefinite censorship compelling digital resilience**

The Uganda Communications Act 2013 allows for censorship discretion in the name of public order and national security. UCC lifted the Internet ban a few days after announcing the 2021 election results but has since continued blocking Facebook to date (Solomon et al., 2024). Amid Internet restrictions and censorship, Ugandan civil society organisations are using KoboToolbox and KoboCollect to document human rights abuses and violations.

KoboToolbox and KoboCollect's offline functionality boosts the resilience of civil society organisations to internet restrictions and shutdowns (Kobo, 2023; Maxwell Maseko, 2023). Human rights reporting on the 2021 and 2026 general elections also pointed to the important role KoboToolbox/KoboCollect and similar technologies have played in civil society organisations' (CSOs) digital resilience in Uganda's restrictive working environment (Kobo, 2023; Kibukamusoke, 2022). Civil society actors and human rights organisations working in fragile, remote and low-internet-access environments have also raised concerns. For example, the Uganda Red Cross Society collected data on flash floods and landslides, drought precursors and COVID-19 cases in remote districts such as Bukedea and Bulambuli (Red Cross Society, 2022).

Civil society actors on the ground use digital documentation tools and circumvention technologies to combat poor internet access and censorship. Civil society organisations in third countries have used VPNs and ODK-based documentation tools such as KoboToolbox and KoboCollect to stay resilient during internet shutdowns and limited connectivity (Loola Bokonda et al., 2020).

**4.6.2. Uganda Communication Act 2013: Sections 79 and 80**

Sections 79 and 80 of the Uganda Communications Act (2013) can strengthen the telecommunications regulatory framework and indirectly support human rights organisations. They criminalise privacy violations in Uganda and penalise service providers for illegal interception and disclosure of communications. The pecuniary penalties of the two sections may have effect on the petty offenders but the fines are for the major offenders. However, large sources of income or prudent use of fines rather than jail time keep the powerful insulated from prosecution. The big problems are their broad discretionary powers and the uncertainty over how they will be implemented.

Sections 79 and 80 of the Uganda Communications Act 2013 provide for the interception and disclosure of communications. Section 79 of the Uganda Communications Act 2013 provides as follows:

*"(1) Any operator of a communications service or system, or any employee of an operator of a communications service or system, who-*

*(a) intercepts the communication of any other person being transmitted by means of that service or system without the consent of the sender or the receiver thereof;*

*(b) willfully or maliciously interferes with or obstructs any radio communications; or (c)*

*(c) reveals any information relating to a communication of which it is aware, commits an offense and is liable on conviction to a fine not exceeding one hundred and twenty currency points or to imprisonment not exceeding five years or to both.*

*(2) A person who, without lawful excuse, intercepts, makes use of or divulges any communication, except where permitted by the originator of the communication, commits an offense and is liable on conviction to a fine not exceeding one hundred and twenty currency points or to imprisonment not exceeding five years or to both such fine and such imprisonment.*
*(3) For the purposes of sub-clause (2), where the subsequent conviction is a subsequent conviction, the person shall be liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or to both."*
Section 80 of the Uganda Communication Act 2013 complements section 79 with further provisions on the interception of communications of the Government of Uganda. It says:
*(1) Any operator of a communications service or employee of an operator who willfully intercepts, disrupts, denies accessibility to or diverts a government communication commits an offense and is liable on conviction to a fine not exceeding ninety-six currency points or to imprisonment for a term not exceeding forty-eight months or to both.*
These provisions may serve to deter or punish petty offenders but are more likely to be selectively applied in support of state-sponsored communication illegality or against perceived anti-government actors (Fitsanakis, 2003; Sutherland, 2019). The UGX 2.4 million fine (about US$705) for mishandling communications under Sections 79 and 80 of the Uganda Communications Commission (UCC) Act (2013) is a serious concern about its deterrent effect, especially for large telecommunications companies and government institutions, including intelligence agencies. The fine is very small in comparison to the huge revenues of telecommunication companies which are often in the millions of dollars per year or the earnings of the government officials who deliberately order the illegal interception of communications (Nkundabanyanga et al., 2019). As such, these companies and government institutions may view the fine as an operational cost rather than as a serious repercussion of non-compliance. This perception may lead to a culture of complacency where profit maximisation overrides regulatory standards. Furthermore, government agencies that break rules rarely face any financial repercussions, particularly intelligence agencies that use telecommunications for surveillance (Sutherland, 2019). Minimal penalties may encourage these agencies to act with impunity, ignoring citizens' rights to privacy and free expression in pursuit of operational objectives.
The fine also does not take into account the potential damage caused by non-compliance, such as service outages, privacy breaches and infringements on consumers' rights (Sutherland, 2019). The lack of a graduated penalty system, which would increase fines based on the severity or repetition of violations, further undermines regulatory enforcement. The UCC should review the penalty scheme to provide for more substantial, proportionate fines and a graduated penalty system. "This will improve compliance and ensure that both private and public entities are held to the same standards of accountability. Sections 79 and 80 of the Uganda Communications Act (2013) can strengthen the telecommunications regulatory framework and indirectly support human rights organisations. They criminalise privacy violations in Uganda and penalise service providers for illegal interception and disclosure of communications. The pecuniary penalties in the two sections may affect petty offenders, but the fines target major offenders. However, large sources of income or the prudent use of fines, rather than jail time, keep the powerful insulated from prosecution. The big problems are their broad discretionary powers and the uncertainty over how they will be implemented.
Sections 79 and 80 of the Uganda Communications Act 2013 provide for the interception and disclosure of communications. Section 79 of the Uganda Communications Act 2013 provides as follows:

*"(1) Any operator of a communications service or system, or any employee of an operator of a communications service or system, who-*
*(a) intercepts the communication of any other person being transmitted by means of that service or system without the consent of the sender or the receiver thereof;*
*(b) willfully or maliciously interferes with or obstructs any radio communications; or (c)*
*(c) reveals any information relating to a communication of which it is aware, commits an offense and is liable on conviction to a fine not exceeding one hundred and twenty currency points or to imprisonment not exceeding five years or to both.*
*(2) A person who, without lawful excuse, intercepts, makes use of or divulges any communication, except where permitted by the originator of the communication, commits an offense and is liable on conviction to a fine not exceeding one hundred and twenty currency points or to imprisonment not exceeding five years or to both such fine and such imprisonment. 50Act 1 Communications Act, 2013 Uganda.*
*(3) For the purposes of sub-clause (2), where the subsequent conviction is a subsequent conviction, the person shall be liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or to both.*"

Section 80 of the Uganda Communications Act 2013 complements section 79 with further provisions on the interception of Government of Uganda communications. It says:

(1) Any operator of a communications service or employee of an operator who willfully intercepts, disrupts, denies accessibility to or diverts a government communication commits an offense and is liable on conviction to a fine not exceeding ninety-six currency points or to imprisonment for a term not exceeding forty-eight months or to both.

These provisions may deter or punish petty offenders but are more likely to be applied selectively to support state-sponsored communication illegality or to target perceived anti-government actors (Fitsanakis, 2003; Sutherland, 2019). The fine of UGX 2.4 million (USD 705) for mishandling communications under Sections 79 and 80 of the Uganda Communications Commission (UCC) Act (2013), raises serious questions about its deterrent effect, particularly among large telecommunications companies and government institutions, including intelligence agencies. The fine is very small in comparison to the huge revenues of telecommunication companies which are often in the millions of dollars per year or the earnings of the government officials who deliberately order the illegal interception of communications (Nkundabanyanga et al., 2019). As such, these companies and government institutions may view the fine as an operational cost rather than as a serious repercussion of non-compliance. Such a view can encourage a complacent culture in which the objective is profit maximisation and not complying with regulatory standards. Further, government agencies that violate the rules usually face no financial consequences, especially intelligence agencies that use telecommunications for surveillance (Sutherland, 2019). Minimal penalties may encourage these agencies to act with impunity, ignoring citizens' rights to privacy and free expression in pursuit of operational objectives.

The fine does not account for potential harm from non-compliance, such as service interruptions, privacy breaches, and violations of consumers' rights (Sutherland, 2019).

The lack of a graduated penalty system to increase fines for more serious or frequent violations further hampers regulatory enforcement. The UCC should review the penalty scheme to provide for more substantial, proportionate fines and a graduated penalty system. "This will improve compliance and ensure that both private and public entities are held to the same standards of accountability.

### 4.6.3.Uganda Communication Act 2013: Section 86-Contextual Censorship

The Uganda Communications Commission (UCC) under section 86(1)(a) of the Uganda Communications Act 2013 can "direct" network operators to behave in a certain way. This is particularly useful in an emergency situation. African governments have exploited the pretext of "states of emergency" to shut down and censor the Internet to control the flow of data and hide problems of bad governance and accountability (Bergère, 2020). Governments turn off the internet to silence political opponents and those fighting for human rights. In the 2011, 2016 and 2021 elections in Uganda, these sorts of reasons were used to shut down the Internet and social media for everyone or even just some people. This was to keep a lid on the violence and chaos that came with the elections. "Freedom to live is more important than the freedom to express oneself," said the Executive Director of the Uganda Communications Commission (UCC). This is typical of some government officials who prefer the safety of the public to civil liberties.

Orders to cut off access to social networks and the Internet to protect public safety and order highlight a reason for censorship that makes sense during times of political unrest and social unrest (CIPESA, 2014). UCC orders are hard to track down because they are often contested in court. Some providers did not comply with the directive to block access to violent social media messages during "Walk to Work" in 2011, as they received the messages after the 24-hour period had elapsed (American Center for Media Excellence, 2011). Then there was a new wave of more advanced government surveillance and monitoring. This is also supported by the reports of Privacy International (2015) on the Uganda Police Force and the plans of the Office of the President to buy high-tech surveillance equipment from Israel and Italy. Concerns were raised as the Ugandan government began to engage in wide-ranging invasive practices. The government employed censorship and intimidation against opposition voices and civil society, among other means to silence dissent during the 2016 election season. UCC fully implemented orders to block Facebook, WhatsApp and Twitter a day before and on the day of President Museveni's inauguration in May 2016 (CIPESA, 2016). The fact that in Uganda censorship and surveillance go hand-in-hand makes the human rights situation complicated. When there is no balance between state security, public order and digital privacy, things can quickly turn authoritarian. To monitor, record and report human rights constantly (Nandy, 2023), human rights organizations need to use safe, new technologies.

The government has not ceased in its quest for more sophisticated intelligence tools. There is little research on what the government can do with intelligence, but the statewide internet blackout before the January 2021 elections shows that UCC powers are strictly enforced when needed (APC, 2021). The fact that in 2021 the internet was shut down for five days is testimony to the authority that the Uganda Communications Commission (UCC) had over phone companies and over data flows in Uganda. The Ugandan government often showers praise on the Uganda Communications Commission (UCC) for its ability to monitor and improve communication infrastructure. However, human rights groups and international human rights bodies have criticised the UCC as an oppressive tool that limits freedom of choice (Walyemera, 2021).

### 4.7. Data Protection and Privacy Act 2019 (DPPA)

The Ugandan government has been lauded for enacting the Data Protection and Privacy Act 2019 (DPPA 2019) to protect data and privacy, despite shortcomings in addressing targeted or mass surveillance, illegal digital intrusion, and the new challenge of Artificial Intelligence (Ronald, 2026). Studies show that most data protection and privacy laws focus more on security than on privacy because drafters believe State interests outweigh individual, group, and organisational privacy (Westerlund & Enkvist, 2016). Uganda's

Data Protection and Privacy Act 2019 (DPPA 2019) follows suit by emphasising data protection rather than digital privacy protection. However, DPPA 2019 focuses on data management and security, but its scope is limited in addressing the wider implications for individual privacy, prompting a critical analysis of its overall impact on data protection rights.

Uganda's Data Protection and Privacy Act 2019 (DPPA 2019) is a positive step toward safeguarding the digital privacy of individuals, groups, and organisations. DPPA 2019 lays down data management processes, data security, consent, data audits, data assessments, complaint management, etc. Although data protection and privacy legislation is well-intentioned, research shows friction between State surveillance practices and digital privacy protection (Kumari, 2026), resulting in crimes, human rights abuses and human rights violations.

**4.7.2.Offences and penalties under DPPA Sections 35-38**

Sections 35, 36, 37, and 38 of the Data Protection and Privacy Act 2019 specify offences and detail the consequences of non-compliance, thereby creating a comprehensive framework for enforcing data protection regulations (Blazevic et al., 2021). These sections are essential to holding organisations accountable for their data management policies and ensuring individuals' privacy rights are prioritised. The Act defines specific breaches, clarifies what constitutes an offence, supports compliance, and reduces misunderstandings about organisational obligations.

The offences under this act include unlawful data obtention and disclosure, unlawful data destruction, unlawful data deletion, data concealment, data alteration and sale of personal data. Unlawful data obtention and disclosure refers to the unauthorised acquisition of personal data and its subsequent sharing without the individual's consent. Unlawful data destruction and unlawful data deletion are also critical offences outlined in the Act. The intentional or negligent act of destroying or deleting personal data without following the established legal protocols can lead to irreparable harm for individuals whose data is mishandled. Data concealment involves deliberately hiding or misrepresenting personal data, while data alteration involves unauthorised modifications to existing data. Both actions can cause significant misinformation and misuse of personal data, jeopardising individuals' rights and safety. The sale of personal data is a particularly egregious offence that raises significant ethical concerns. Many brokers and Android applications in developing countries and the European Union zone transfer individuals' personal information to third parties, often for profit, without the individuals' explicit consent (DiPersio, 2024; Nguyen et al., 2021). Such actions breach informed consent principles and expose individuals to risks such as identity theft and targeted exploitation.

The significance of these offences is amplified by the increasing reliance on data for various purposes, including research, marketing, and service delivery. In the digital era, responsible management of the data lifecycle (from collection to deletion) is essential to maintain data integrity and safeguard individual rights. The Data Protection and Privacy Act 2019 imposes substantial penalties for those convicted of such offences and empowers regulatory bodies, especially the Data Protection and Privacy Office (DPPO), to enforce them. An individual convicted of any of the above offences may face a fine not exceeding two hundred and forty-five currency points (UGX 4,800,000), imprisonment not exceeding ten years, or both (Grant Thornton, 2021). Section 38 of the Data Protection and Privacy Act 2019 imposes hefty penalties on corporations and their staff who knowingly and willfully authorise or allow data protection and privacy breaches. In addition to the punishment, the Data Protection and Privacy Act 2019 obliges the convicted corporations and their staff to pay a fine not exceeding two per cent (2%) of the corporation's annual gross turnover (Idem)

### 4.7.3. DPPA Section 10: sole mention of privacy over data protection provisions

The Data Protection and Privacy Act of 2019 has drawn substantial criticism for emphasising data protection over a more holistic approach to privacy rights, as only one section (Section 10) of its 40 sections addresses privacy protections. Section 10 of the Act reads, "*A data collector, data processor, and data controller shall not collect, hold or process data in a manner which infringes on the privacy of a data subject*." Digital rights specialists contend that this disproportionate focus treats digital privacy rights as mere elements of digital data security rather than inherent rights, thereby exposing human rights organisations to unlawful surveillance and privacy violations under the pretext of national security and public order (Hiranandani, 2011). The Data Protection and Privacy Act 2019 (DPPA 2019) fails to set out clear provisions on crucial aspects of privacy protection, such as the use of encryption-enabled tools, opening the door for human rights violators and abusers to intrude into digital privacy with impunity. Although Section 10 encourages organisations to adopt robust security measures to protect individuals' privacy, explicit legislative provisions provide clear guidance for drafting regulations (Xanthaki, 2014) and set rules for implementation and enforcement. Despite these arguments and counter-arguments, the Data Protection and Privacy Act 2019 safeguards data subjects from data collectors, controllers, and managers. Therefore, Section 10 requires the latter to collect, share, store, and manage data in a way that respects the privacy of data subjects (individuals). This means data collectors, controllers, and managers must uphold confidentiality and protect data subjects' identities and personal information throughout the data lifecycle and documentation processes.

The Data Protection and Privacy Act 2019 does not cover the security and privacy of data collectors, controllers, and managers, including telecommunication companies, researchers, human rights organisations, and individual human rights defenders. The sensu stricto definition of data management privacy focuses on obtaining consent from data subjects, the stages of the information cycle (including data collection and management), and the legal obligations of data managers (Wodi, 2023). In contrast, the sensu lato perspective broadens this notion to include privacy as a fundamental freedom against unjust intrusions and surveillance by state and non-state actors, and the right to use digital security measures to safeguard against privacy-infringing technologies in the digital environment. More than 100 countries, including Uganda, have enacted laws that intertwine privacy and data protection (Banisar, 2016), giving security agencies room to use intelligence and political clout to target organisations and individuals with privacy-enabled tools (Banisar & Davies, 2012). Protection law should be separated from privacy law to avoid endless pretexts for violating and abusing digital privacy and rights in the name of national security and public interest, and to hold organisations and the government equally accountable.

Data and privacy protection laws are interconnected and often overlap, yet they serve three distinct purposes. While privacy law focuses on individuals' and entities' rights to control data and information and to protect confidentiality and private lives (Jagannadh & Sumitra, 2025), data protection law sets out regulatory frameworks for handling individuals' and entities' data and information (Pande, 2026). Privacy law encompasses broader issues beyond data, including individuals' and entities' autonomy and freedom from surveillance, whereas data protection law specifically addresses the collection, processing, and security of personal data (Fuster & Bellanova, 2013). Data protection laws include specific compliance requirements for organisations. In contrast, privacy laws may address organisations' and individuals' rights and freedoms regarding surveillance and invasions.

### 4.7.4. The Data Protection and Privacy Regulations 2021 and Office

The European Union General Data Protection Regulation (GDPR) has inspired all the data and privacy protection laws in most countries, including Uganda. Uganda's Data Protection and Privacy Regulations 2021 and its Data Protection and Privacy Office (DPPO) are more or less copy-and-cat structures of the European Union. However, the GDPR and Data Protection Regulation 2021 lack concrete measures on data privacy (Vanberg, 2021), which cannot hold organisations and states accountable equally. GDPR and are still new legislations. They have embarked on a protracted legal road with numerous trials and errors, lacking precise provisions about rights and freedoms to address violations and abuses resulting from States and corporations. The Personal Data Protection and Privacy Office (PDPPO), under the oversight of NITA-U, has been praised for introducing and enforcing data protection privacy regulations in Uganda(Personal Data Protection Office, 2025). DPPO has accomplished milestones such as automating data controller registration, complaint filing, and breach reporting. The office has also organised over 100 awareness initiatives aimed at Government ministries, departments and agencies (MDAs), private sector entities, civil society organisations, development partners, professional and business associations, educational institutions, and the general public. Moreover, it has facilitated 14 capacity-building sessions for data protection officers, finalised three (3) compliance audits, and registered over 2,900 regulated individuals. It has conducted data protection and privacy awareness-raising campaigns [1]using various channels such as audio-visual media and marathons (Personal Data Protection Office, 2024).

Despite the Personal Data Protection Office (PDPO)'s achievements in enhancing data protection and privacy standards in Uganda, several challenges that could undermine its effectiveness persist. Although the PDPO has established compliance frameworks and conducted audits, many organisations, particularly community-based and under-funded organisations, may lack the resources or expertise to comply fully, leading to inconsistent practices and increased risks of data breaches(Bwire, 2023). Compliance remains a fundamental pillar for the sustainability and integrity of organisations, particularly for small enterprises that often grapple with limited financial resources and a scarcity of technical expertise. In Uganda, as in many jurisdictions, the landscape of regulatory requirements—including data protection laws—continuously evolves, presenting significant challenges for these smaller organisations. They may struggle to implement effective compliance measures without the necessary funding or specialised knowledge, leaving them vulnerable to legal repercussions and potential reputational damage. In light of the above predicament, PDPO organised a workshop for financial technology corporations (FinTechs) and micro, small and medium enterprises (MSMEs) to get insights on tailored support systems and resources that can empower small organisations to navigate the complexities of compliance, fostering a more equitable business environment and enhancing overall governance in data and privacy protection(Personal Data Protection Office | PDPO - UG, 2024). Privacy and data protection authorities and other big data institutions face many challenges from emerging technologies, particularly artificial intelligence (AI). As these technologies grow, data handling, processing, and misuse become more complex, requiring regulatory authorities to be proactive and adaptable (Singla, 2024). The PDPO, like its global like-minded institutions, finds it challenging to update its principles and policies to accommodate these improvements and preserve private rights. Uganda's Personal Data Protection Office (PDPO) enforcement efforts are far better than those of other privacy and data protection offices in Kenya, Mauritius, and Zimbabwe (UnwantedWitness, 2023). However, the PDPO, like other government institutions in Uganda, has limited

[1] https://www.pdpo.go.ug/news/pdpo-unveils-the-2024-data-privacy-campaign

staffing and funding, which can restrict its ability to monitor compliance, enforce regulations, and address complaints effectively. In her analysis of the national impacts of adopting European data and privacy standards, Sivan-Sevilla (2022) found that the lack of sufficient human, financial, and technical resources in the operational capabilities of privacy and data protection bodies raises concerns about their ability to enforce compliance and safeguard digital privacy rights.

The designation of the Personal Data Protection Office (PDPO) raises significant concerns regarding privacy rights, particularly given that the name of this important office lacks an explicit reference to privacy, which may lead to public confusion about its mission and authority. This discrepancy is notable in light of the explicit provisions for privacy outlined in the Data Protection and Privacy Act of 2019 and the Data Protection and Privacy Regulations of 2021, which mandate the safeguarding of personal data and the protection of individual privacy rights. The absence of a clear emphasis on privacy in the data and privacy institutions' names could undermine public confidence in its capacity to effectively enforce these legal frameworks and protect citizens' rights, thereby highlighting the need for a more coherent alignment between institutional branding and legislative intent in the realm of data protection and privacy (Srivastava & Siddiqui, 2024). Studies have shown that data and privacy protection laws influenced by the EU General Data Protection Regulation (GDPR) have faced the challenges of misaligning the names and the laws they intend to enforce and implement, as governments are reluctant to empower data and privacy protection bodies to tackle State surveillance and invasion of communications or State-sanctioned privacy violations and abuses (Bharti & Aryal, 2022). Judijanto et al. (2024) recommend that governments address misnomers and vagueness in defining data protection, digital security, and privacy to provide clear enforcement guidelines and powers for privacy and data protection oversight bodies.

### 4.8. State obligations to Protect Digital Privacy right in Uganda

#### 4.8.1. Obligations to respect, protect and fulfil digital privacy enjoyment

Uganda is a signatory to international human rights treaties and agreements, and the Government of Uganda must respect, protect, and fulfil human rights. This section sets out the extent to which the Government of Uganda has upheld its obligations (Respect, Protect, and Fulfil) regarding the digital privacy of civil society organisations. Police raids and the seizure of digital devices are among the unwarranted invasions of privacy that Ugandan human rights organisations have faced. Another sign that human rights organisations' digital privacy is not protected is the delay or non-release of reports on investigations into the hacking of organisational computers.

#### 4.8.2 Obligation to respect the enjoyment of digital privacy

##### 4.8.2.1. Digital privacy interference using legal channels

Human rights groups have pointed out that the Government of Uganda has used legal means, such as police raids, to interfere with people's right to digital privacy. Yeon (2021) and Pool (2017) highlight the possibility of privacy violations through police searches of digital devices and computer hacking. The Uganda Police Force (UPF) was authorised to raid ActionAid Uganda and the Great Lakes Initiative for Strategic Studies (GLISS) to confiscate computer accessories (electronics) and mobile handsets (Daily Monitor, 2017). Police seized computers, servers and phones for analysis. The Uganda Human Rights Commission (UHRC) says the inspection of the confiscated electronics was transparent because it was carried out without ActionAid Uganda and GLISS staff. Police violate digital privacy during raids, which creates suspicion between government institutions and human rights organisations (Lorjé, 2021). The UHRC has observed that invasions of human rights organisations' digital privacy, with or without a warrant, remain a persistent human rights issue globally and in Uganda.

The government has been too intrusive in hacking into people's computers, which has led to increased use of encryption-enabled technology such as KoBo Toolbox (Škorvánek, 2019). The Uganda Human Rights Commission (UHRC) took on the position of the National Information Technology Authority (NITA), security agencies, and some government officials who reject the idea of 'My Computer is my inviolable castle' by human rights organisations. "Security services, NITA and some government organs believe human rights organisations should be protected from the intrusion of non-state actors," the UHRC said. They say these human rights organisations should not withhold information from the government responsible for granting human rights, including digital privacy rights. The UHRC concurred with human rights organisations that existing laws and policies, including the Data Protection and Privacy Act 2019 and the Data Protection and Privacy Regulations, do not grant human rights organisations the right to use encryption and other tools to protect their digital privacy from intruders, whether State or non-State actors.

**4.8.2.2 Digital privacy interference via masqueraded office break-ins**

Human rights organisations use KoboToolbox, KoboCollect, and other encryption-enabled tools because they fear office break-ins and theft targeting their digital data. They have experienced such attacks since 2014, as the Uganda Human Rights Commission explained (Commission, 2014). UHRC described these recurring break-ins of human rights organisations as human rights concerns. It reserved a section in the 2018 annual UHRC report to underscore these concerns; UHRC was reluctant to qualify the office break-ins as a State-sponsored invasion of human rights organisations' digital privacy.

Various concerns regarding digital privacy rights have been raised, citing reports from the Uganda Human Rights Commission (UHRC), media outlets, and other human rights organisations. In 2014, the Human Rights Network-Uganda (HURINET) office was broken, which resulted in the theft of one (1) and twenty-nine (29) computers (Uganda Human Rights Commission, 2018). During the same year, other organisations, including Women and Girl Child Development, Action Group for Health Advocacy, AFFORD Kasese, Human Rights Focus Uganda (HURIFO) and Ecological Christian Organisation, faced the same fate (Idem). In 2015, there were other reports of burglaries targeting digital data at Uganda Land Alliance, Anti-Corruption Coalition, Human Rights Network for Journalists – Uganda (HRNJ), and Foundation for Human Rights Initiative (Idem). In 2018, the offices of Karambi Action for Life Improvement (KALI), Isis-Women's International Cross-Cultural Exchange (Isis WICCE) and Human Rights Awareness and Promotion Forum (HRAPF) were broken into (Uganda Human Rights Commission, 2018). Instead of handling the issues of invading human rights organisations' digital privacy comprehensively, the government of Uganda has continuously implemented measures to shut down the Internet, surveil targeted online users and increase data espionage (Davis, 2019; Selne, 2020). The 2021 Internet outage and subsequent Facebook blockage clearly demonstrate the Ugandan government's infringement of Internet rights, particularly digital privacy rights (Uganda Human Rights Commission, 2021).

The Uganda Police Force has not published reports on these office break-ins despite calls from human rights organisations, the Uganda Human Rights Commission, and United Nations human rights bodies. The Uganda Human Rights Commission and human rights organisations have noted that the office break-ins and police raids have raised suspicions within the government, particularly among security services, and among human rights organisations. Human rights organisations have raised fears that the Ugandan government may be responsible for the office break-ins to access organisations' digital data, given its unwillingness to address these recurring human rights issues.

### 4.8.3 Obligation to protect the enjoyment of digital privacy

#### 4.8.3.1 Incomplete responsive interventions to digital privacy invasion

The Government of Uganda has been called upon repeatedly to address concerns about digital privacy rights following break-ins at human rights organisations' offices. However, human rights organisations and the Uganda Human Rights Commission (UHRC) have expressed concern over the government's response to the break-ins, claiming the interventions were incomplete and inadequate (Freedom House, 2016). They say the interventions have been marked by a lack of accountability, with a tendency to dodge responsibility and place blame. According to Brehm (2011), avoiding responsibility includes strategies politicians and bureaucrats use, such as lies, misleading statements on hot topics, and various misattributions of responsibility.

The puzzle of human rights concerns about the human rights organisations' office break-ins started in 2014 when a group of human rights organisations issued a statement titled 'Civil *Society Office Break-ins in Uganda: The Unanswered Questions*[2]'. Despite constructive dialogue meetings between the Ministry of Internal Affairs and civil society organisations, the Government of Uganda has failed to dispel suspicions that state agencies and their proxy thieves are behind the human rights office break-ins (Human Rights Watch, 2021). Participants in the June 2024 dialogue urged the Government of Uganda, through the Uganda Police Force (UPF), to produce reports on office break-ins targeting human rights organisations to allay civil society organisations' suspicions. They also acknowledged that the Uganda Human Rights Commission (UHRC) dedicated an entire section of its 2018 report to office break-ins to highlight these digital rights concerns. (Uganda Human Rights Commission, 2018). Similarly, Human rights organisations and UN human rights bodies have indicated that the Ugandan government has neglected its obligations to investigate and report on break-ins that specifically target the digital privacy of over 30 human rights organisations (CIVICUS, 2018). Since 2018, in the constructive dialogues involving the Ministry of Internal Affairs, the National Bureau for Non-Governmental Organisations, civil society organisations (CSOs), security agencies such as the Uganda Police Force (UPF), government officials from various ministries, the diplomatic corps, parliamentarians and other stakeholders, the failure was discussed, but the government of Uganda became defensive (Human Rights Centre Uganda, 2023) and requested more time to conclude the investigations into break-ins at NGOs' offices.

Human rights advocates and scholars decry the Government of Uganda's failure to investigate office break-ins targeting digital devices as a deliberate move to invade civil society organisations' privacy. The lack of accountability and persistent impunity for attacks on human rights defenders and their offices sends a message that authorities condone and tolerate such attacks(Amnesty International, 2016). During the June 2024 dialogue meetings and similar dialogues in 2023 and 2022, the representatives shifted blame to UPF area commanders. Civil society organisations were assured that "*UPF would direct its area commanders to conclude investigations into all office break-ins reported by human rights organisations since 2014"*. Human rights organisations and scholars argue that the blame game and long-time avoidance show that the Government of Uganda prioritises political power over digital privacy, and they constitute indicators of a violation of fundamental human rights, as security and privacy are essential for the exercise of constitutional rights (Dragu & Lupu, 2021)

[2] https://www.monitor.co.ug/uganda/magazines/people-power/who-could-be-breaking-into-ngos-offices--1572986

#### 4.8.3.2. No preventive interventions for digital privacy violations

The State's obligation to protect requires proactive interventions to prevent State and non-state actors from invading human rights organisations' digital privacy. States must inform human rights organisations about risks and threats to their digital privacy, strengthen these organisations' capacity to defend against digital privacy attacks, and implement initiatives that promote practices that protect digital privacy. Instead of adopting laws designed to prevent digital privacy attacks, the Government of Uganda has enacted privacy-invasive legislation that undermines the very rights it purports to protect (Muhangi, 2019). This legislative strategy illustrates a concerning trend in which laws purportedly designed to safeguard national security or public order are used to rationalise widespread surveillance and infringe on individual privacy rights.

Governments have enacted legislation requiring telecommunications providers to store metadata on citizens' emails, text messages, and phone calls for up to two years (Sarre, 2017). These records must be accessible to national security services for investigative purposes. Few governments, including Uganda's, have implemented some measure measures to prevent state actors from invading digital privacy (The Republic of Uganda, 2019). When questioned about the efforts made by the Government of Uganda to raise awareness about the importance of protecting digital privacy, the Uganda Human Rights Commission (UHRC) and the National Information Technology Authority (NITA) referred to the Computer Misuse Act and other laws, which grant excessive authority to security services to infringe upon digital privacy.

The Ugandan government has not put in place systematic, coordinated mechanisms to educate the public and human rights organisations on using encryption-enabled tools to protect digital privacy. The Uganda Human Rights Commission (UHRC) stated that "*it lacks the technical expertise in digital privacy and computer science to offer guidance and remedies to human rights groups whose digital privacy can be breached by both State and non-state actors*". The Uganda Human Rights Commission (UHRC) recognises the importance of secure digital data-collection tools in improving the documentation of human rights violations. It is eager to forge strategic alliances with the developers of these technologies. The Research, Education and Documentation Directorate of UHRC has used KoboToolbox and Kobo Collect to collect field data securely across the country. The UHRC team believes that *secure digital innovations such as KoboToolbox and KoboCollect protect digital privacy, and UHRC uses KoboToolbox and KoboCollect in its studies on sensitive human rights issues.* UHRC plans to collaborate with technology developers to leverage advanced digital tools to facilitate the collection, analysis, and preservation of evidence related to human rights abuses, thereby strengthening the accountability mechanisms within the country.

Additionally, UHRC said these collaborations should include academia to build a local pool of experts and develop best practices and guidelines that ensure the ethical use of technology in human rights documentation. Ultimately, this strategic engagement with technology developers reflects a forward-thinking approach that recognises the intersection of human rights and technology, paving the way for more effective advocacy, secure evidence capture, and the protection of human rights and fundamental freedoms in Uganda.

### 4.8.4. Obligation to fulfil the digital privacy enjoyment

#### 4.8.4.1. Implicit constitutional and legal protections of digital privacy

The Government of Uganda has adopted legal provisions to protect the right to privacy.

The Uganda Human Rights Commission (UHRC) and the National Technology Authority (NITA) stated that the supreme law of Uganda stipulates in its Article 27 (2), "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property"

(Uganda Constitution, 1995). According to the UHRC and NITA, the Uganda Constitution does not explicitly address digital privacy because it was created before the digital era became widespread globally. At the time, no legal precedent or established policy addressed digital privacy. Moreover, the lawmakers lacked expertise and experience in the digital domain. However, the Uganda Constitution was drafted with remarkable foresight, as it explicitly addressed digital privacy by prohibiting any unlawful interference in correspondence, communication, and property. The communication, correspondence and property can be both physical and digital. Ivanov (2023) and Michels (2022) contend that policymakers and legislators see the potential for digital correspondence, such as emails, to act as a form of physical communication. Similarly, they acknowledge that digital tools, such as computers and servers, can function as a type of physical property. Traditional law principles protect digital communication, correspondence, digital assets, and digital content. The UHRC and NITA emphasised that the Government of Uganda has enacted several laws on digital privacy and data protection, including the 2011 Computer Misuse Act, the 2010 Regulation of Interception of Communication (RICA), and the 2019 Data Protection and Privacy Act, to protect data and privacy.

However, they recognised that current legislation in Uganda fails to grant individuals the rights and freedoms needed to safeguard their digital privacy, including the rights to use encryption and maintain online anonymity, as well as freedom from surveillance and defamation. While UHRC and NITA assert that section 10 of the 2019 Data Protection and Privacy Act protects digital privacy, this law primarily addresses the obligations of data collectors, processors, and storers, rather than explicitly protecting individuals' or data subjects' digital privacy rights. Existing laws and policies (as discussed in Chapter Four: Critique on digital privacy laws and policies) emphasise digital security and safety. As a result, human rights organisations distinguished digital privacy from digital protection in sections 8 and 9 of the Charter of Human Rights and Principles for the Internet (Internet Rights & Principles Coalition, 2014). This distinction was made to prevent confusion between digital privacy and digital protection. Similarly, the United Nations General Assembly passed resolution 68/167, urging member states to balance individual digital privacy protection with cybersecurity (Global Privacy Assembly, 2014). All United Nations member states, including Uganda, clearly prefer cybersecurity over individual digital privacy (UN Internet Governance Forum, 2023).

**4.8.4.2. Invasive state-sanctioned telecom practices and Internet laws**

Surveillance and the interception of communications have existed since the beginning of time to protect national sovereignty and ensure national security. The Uganda Human Rights Commission (UHRC) and the National Information Technology Authority (NITA) are aware of cases of invasions of individuals' digital privacy, including those involving high-ranking officials and human rights organisations. They argued that digital privacy violations are not limited to Uganda. Following the 1885 Telegraph Act and India's 2009 Information Technology (IT) Act, state security services have the legal authority to limit the transmission of communications, intercept and monitor communications, and decode information using tools, including computers. The UHRC recognised that the Ugandan government has emulated other nations by implementing specific legislation, such as the Computer Misuse Act and the Regulation of Interception of Communications Act, to infringe upon digital privacy.

The Uganda Human Rights Commission (UHRC) stated that Ugandan legislators, politicians, human rights organisations, and academia lack the necessary skills to analyse bills before parliament enacts them effectively. The UHRC cited the Regulation of Interception of Communications Act, tabled by the Prime Minister (Amama Mbabazi), and noted that the same law was used to violate his digital privacy rights.

The Uganda security services used this law to record private conversations between the Prime Minister and his wife (Global Information Society Watch, 2014). In response to the rampant digital privacy violations, the Uganda Human Rights Commission (UHRC) supported discussions on data protection and privacy. The Ugandan Parliament has disclosed the Data Protection and Privacy Bill for public input. UHRC conducted multiple seminars and engagements with human rights organisations and academics, including professors from Makerere University, to gather input for the Data Protection and Privacy Bill. However, stakeholders failed to acknowledge that the bill addressed only data protection and did not include safeguards for digital privacy. Contrary to the Uganda Constitution, the UHRC concurred that Uganda's computer and Internet legislation focuses more on punishment than on granting rights.

### 4.9. Conclusion

Laws and policies are in place to protect digital privacy in Uganda. However, the enjoyment of digital privacy remains limited. Several provisions of the legal and policy frameworks discussed above are vague and open to misinterpretation and misapplication. The Computer Misuse Act (2011) grants government organs unchecked powers to arrest, detain, and prosecute anyone suspected of publishing or possessing offensive communications.

The Regulation of Interception of Communications Act (2010) and the Computer Misuse Act (2011) are open to selective application and unchecked interpretation by security services.

The National Information Technology Authority (NITA) - Uganda Act (2009) provides guidance and regulations on the use of Information and Communication Technology (ICT).

It is supposed to raise awareness of ICT compliance and security issues. The NITA Act grants government agencies much-unfettered discretion. The Anti-Money Laundering Act (2013) deals with illegal money transfers. This law requires human rights organisations and development agencies to submit confidential donor and beneficiary information to the government. Some provisions are prone to misapplication and misinterpretation, targeting the digital privacy of human rights organisations, activists, and development agencies working on government accountability.

The Uganda Communications Act (2013) controls communications. It provides the State with broad, discretionary powers to grant and revoke licenses to mainstream and online media, impose shutdowns, and restrict discussion of specific topics. Unchallenged discretion granted under the Uganda Communications Act and other laws leads to covert surveillance and undue self-censorship. The Data Protection and Privacy Act (2019) governs data use and protection in Uganda. Nevertheless, on digital privacy, the Data Protection and Privacy Act does not address the security and safety of data at rest and in motion, nor does it protect human rights organisations' and activists' rights to use encryption to protect their data and themselves.

### 4.10. Recommendations

1. Amend or repeal the restrictive and ambiguous provisions of the existing digital privacy laws, especially the Computer Misuse Act, that allow legal overbreadth and selective enforcement.
2. Amend the Regulation of Interception of Communications Act 2010 to regulate the State's surveillance powers in line with international human rights standards.
3. Enact a standalone digital privacy protection law to provide explicit guarantees to the rights holders to use privacy-preserving tools such as encryption, anonymity and secure applications and to address gaps in the Data Protection and Privacy Act (DPPA) 2019.

4. Enhance the independence and capacity of the Personal Data Protection Office (PDPO) and Uganda Human Rights Commission (UHRC) to monitor compliance, conduct audits, investigate digital privacy and security violations and abuses and enforce sanctions without political influence.
5. Establish the accountability and oversight mechanisms over the surveillance and privacy invasion operations of State security agencies to ensure transparency and deal with impunity.
6. Support the collaboration between State agencies and civil society to enhance trust in the protection and promotion of digital and digital privacy rights.

**References**

1. American Journal of International Law. (2017). *Recommendation on Inviolability of Postal Correspondence*. https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/recommendation-on-inviolability-of-postal-correspondence1/DC4C43ECA900606862AA19CB60E67316
2. Amnesty International. (2016). *Uganda: Investigate Break-ins at Groups' Offices*. https://www.amnesty.org/en/latest/press-release/2016/06/uganda-investigate-break-ins-at-groups-offices/
3. Banisar, D., & Davies, S. (2012). Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *The John Marshall Journal of Computer and Information Law*, *18*, 1–111. https://api.semanticscholar.org/CorpusID:147389751
4. Basimanyane, D. (2025). *The peril of digital privacy and free speech in Uganda*.
5. Basu, S., & Sen, S. (2024). Silenced voices: unravelling India's dissent crisis through historical and contemporary analysis of free speech and suppression. *Information & Communications Technology Law*, *33*(1), 42–65. https://doi.org/10.1080/13600834.2023.2249780
6. Bharti, S. S., & Aryal, S. K. (2022). The right to privacy and an implication of the EU General Data Protection Regulation (GDPR) in Europe: challenges to the companies. *Journal of Contemporary European Studies*, *31*, 1391–1402. https://api.semanticscholar.org/CorpusID:252770562
7. Bruce, A. (2018). *Is Uncle Sam Stalking You? Abandoning Warrantless Electronic Surveillance to Preclude Intrusive Government Searches*. https://doi.org/Bruce, Alexandra, Is Uncle Sam Stalking You? Abandoning Warrantless Electronic Surveillance to Preclude Intrusive Government Searches (January 31, 2017). Available at SSRN: https://ssrn.com/abstract=2909200 or http://dx.doi.org/10.2139/ssrn.2909200
8. Bwire, L. (2023). Challenges in Implementing Data Protection Laws: Lessons Learnt from Developed Countries. *International Journal of Law and Policy*, *8*(1), 28–36. https://doi.org/10.47604/ijlp.1890
9. Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). *Achieving Privacy Costs of Compliance and Enforcement of Data Protection Regulation Background Paper*. http://www.worldbank.org/prwp.
10. Chugh, U. (2023). The Evolution of Privacy Laws in the Digital Age: Challenges and Solutions. *Indian Journal of Law*. https://api.semanticscholar.org/CorpusID:270918361
11. CIPESA. (2018). *Unmasking Digital Security Threats facing Human Rights Defenders in Uganda and Tanzania – Collaboration on International ICT Policy for East and Southern Africa (CIPESA)*. https://cipesa.org/2018/08/unmasking-digital-security-threats-facing-human-rights-defenders-in-uganda-and-tanzania/
12. CIVICUS. (2018). *Authorities fail to investigate break-ins targeting human rights organisations -*

*Civicus Monitor*. https://monitor.civicus.org/explore/authorities-fail-investigate-break-ins-targeting-human-rights-organisations/

13. Commission, U. H. R. (2014). Report 204 Anual Report. In *확인필요*.
14. DiPersio, D. (2024). Selling Personal Information: Data Brokers and the Limits of US Regulation. *LEGAL*. https://api.semanticscholar.org/CorpusID:269950892
15. Dragu, T., & Lupu, Y. (2021). Digital Authoritarianism and the Future of Human Rights. *International Organization*, *75*, 991–1017. https://api.semanticscholar.org/CorpusID:233924123
16. Finn, T., & Prescott, S. B. (2025). The Impact of International Human Rights Law on Digital Privacy in the Era of Mass Surveillance. *Law and Justice Research Journal*. https://api.semanticscholar.org/CorpusID:281352219
17. Fowler, A., & Sen, K. (2010). Embedding the War on Terror: State and Civil Society Relations. *Development and Change*, *41*(1), 1–27. https://doi.org/10.1111/J.1467-7660.2009.01620.X
18. Gopi C.C. (2026). *Lawful Interception , Constitutional Limits : Surveillance and Service Suspension under the Telecommunications Act , 2023*. *December 2023*, 1–4.
19. Grant Thorton. (2021). *Data Protection and Privacy Act: 2019: The implications to your organization*.
20. Greenleaf, G., & Cottier, B. (2020). Comparing African Data Privacy Laws: International, African and Regional Commitments. *SSRN Electronic Journal*, *April*, 18–21. https://doi.org/10.2139/ssrn.3582478
21. Hennig, N. (2018). Privacy and Security Online. In *Library Technology Reports* (Vol. 54, Issue 3).
22. Hiranandani, V. S. (2011). Privacy and security in the digital age: contemporary challenges and future directions. *The International Journal of Human Rights*, *15*, 1091–1106. https://api.semanticscholar.org/CorpusID:144515984
23. Human Rights Watch. (2021). *Uganda: Harassment of Civil Society Groups*. https://www.hrw.org/news/2021/08/27/uganda-harassment-civil-society-groups
24. Ilori, T. (2021). Framing a human rights approach to communication surveillance laws through the African human rights system in Nigeria, South Africa and Uganda. *African Human Rights Yearbook*, *5*, 134–157. https://doi.org/10.29053/2523-1367/2021/v5a7
25. International, P. (2019). *State of Privacy Uganda*. https://www.privacyinternational.org/state-privacy/1013/state-privacy-uganda
26. Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*. https://api.semanticscholar.org/CorpusID:273975258
27. Lowell, K. (2017). Civil Liberty or National Security: The Battle Over iPhone Encryption. *Georgia State University Law Review*, *33*, 485. https://api.semanticscholar.org/CorpusID:158335941
28. Luck, R. (2014). *RICA - walking a fine line between crime prevention and protection of rights : itc law*. https://api.semanticscholar.org/CorpusID:197818147
29. Maneesh, S., & Prodduturi, K. (2025). *Cryptography in iOS : A Study of Secure Data Storage and Communication Techniques*. *16*(1), 1–8.
30. Maret, S. (2011). Introduction: Government secrecy. In S. Maret (Ed.), *Government Secrecy* (Vol. 19, pp. xi–xxx). Emerald Group Publishing Limited. https://doi.org/10.1108/S0196-1152(2011)0000019003
31. Maret, S. (2021). Concealing in the Public Interest, or Why We Must Teach Secrecy. *Secrecy and Society*, *2*(2). https://doi.org/10.31979/2377-6188.2021.020201

32. Micheal Yilma, K. (2017). Digital privacy and virtues of multilateral digital constitutionalism—preliminary thoughts. *International Journal of Law and Information Technology*, *25*(2), 115–138. https://doi.org/10.1093/ijlit/eax001
33. Molly K. Land, & Jay D. Aronson. (2018, April 18). *New Technologies for Human Rights and Practice*. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A6473E8A4F6A9ED12675E54A03318802/9781107179639AR.pdf/New_Technologies_for_Human_Rights_Law_and_Practice.pdf?event-type=FTLA
34. Molly Land, Patrick Meier, M. B. and, & Jacob, E. (2012). *ICT4HR: Information and Communication Technologies for Human Rights*.
35. Moore, A. D. (2007). *Toward Informational Privacy Rights*. https://api.semanticscholar.org/CorpusID:153708368
36. Muhangi, K. (2019). Overview of the data protection regime in Uganda. *Journal of Data Protection & Privacy*, *3*(1), 82. https://doi.org/10.69554/YETP6689
37. Ngamita, R. (2026). *Smart City Surveillance in Uganda*. https://doi.org/https://doi.org/10.19088/IDS.2025.080
38. Nguyen, T. T., Backes, M., Marnau, N., & Stock, B. (2021). Share First, Ask Later (or Never?) Studying Violations of GDPR's Explicit Consent in Android Apps. *USENIX Security Symposium*. https://api.semanticscholar.org/CorpusID:237521976
39. Pandey, H., Lunia, C., & Rathore, E. N. (2024). Navigating the Digital Maze: Privacy and Security Challenges in the Era of Cloud Computing. *International Journal For Multidisciplinary Research*, *6*(3), 1–6. https://doi.org/10.36948/ijfmr.2024.v06i03.23105
40. Personal Data Protection Office. (2024, June 9). *Personal Data Protection Office | PDPO - UG*. https://www.pdpo.go.ug/updates/running-for-privacy-pdpo-staff-champions-data-protection-as-he-conquers-marathons
41. Personal Data Protection Office. (2025, February 7). *Personal Data Protection Office | PDPO - UG*. https://www.pdpo.go.ug/news/personal-data-protection-office-roots-for-inclusivity-as-uganda-celebrates-the-2024-international-data-privacy-day
42. Personal Data Protection Office | PDPO - UG. (2024). *PDPO and FSD Uganda Collaborate to Enhance Data Protection Compliance for FinTechs and MSMEs*. https://www.pdpo.go.ug/news/pdpo-and-fsd-uganda-collaborate-to-enhance-data-protection-compliance-for-fintechs-and-msmes
43. Privacy International. (2015). *For God and My President: State Surveillance in Uganda*. https://privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf
44. Rider, K. (2018). The privacy paradox: how market privacy facilitates government surveillance. *Information Communication and Society*, *21*(10), 1369–1385. https://doi.org/10.1080/1369118X.2017.1314531
45. Rooney, J. (2017). Going Postal: Analyzing the Abuse of Mail Covers under the Fourth Amendment. *Vanderbilt Law Review*, *70*, 1627. https://api.semanticscholar.org/CorpusID:158940652
46. Saki, O. (2025). *' We will visit your bedrooms ': Testing the adequacy of safeguards in the interception of communications in Zimbabwe through the lens of the AmaBhungane case*. *2007*, 822–851.
47. Sampson, S. (2010). Diagnostics: Indicators and Transparency in the Anti-Corruption Industry. *Transparenz*, 97–111. https://doi.org/10.1007/978-3-531-92466-3_7
48. Sarre, R. (2017). *Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia*. https://link.springer.com/article/10.1007/s11417-017-9256-7

49. Schumann, M. P. (2026). Legalizing control: the rise of restrictive internet regulation in sub-Saharan Africa. *Democratization*, *33*(1), 137–162. https://doi.org/10.1080/13510347.2025.2503370
50. Serohin, V. (2021). Information Privacy: a Conceptual Approach. *Constitutional and Legal Academic Studies*, *2*, 52–60. https://doi.org/10.24144/2663-5399.2020.2.06
51. Siegel, D. (2011). Secrecy, Betrayal and Crime. *Utrecht Law Review*, *7*(3), 107. https://doi.org/10.18352/ulr.173
52. Singla, A. (2024). The Evolving Landscape of Privacy Law: Balancing Digital Innovation and Individual Rights. *Indian Journal of Law*. https://api.semanticscholar.org/CorpusID:270126633
53. Solove, D. J. (2005). Access and Aggregation: Privacy, Public Records, and the Constitution. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.283924
54. Srivastava, P., & Siddiqui, S. (2024). DATA PROTECTION IN THE AGE OF SOCIAL REGULATION: A CONCEPTUAL FRAMEWORK. *ShodhKosh: Journal of Visual and Performing Arts*. https://api.semanticscholar.org/CorpusID:274118747
55. Svobodová, T. (2025). *RECALIBRATING LIBERTY AND SECURITY: HUMAN RIGHTS CHALLENGES IN THE AGE OF MASS SURVEILLANCE*. https://doi.org/https://doi.org/10.55843/icl2025cong117s
56. Tactical Technology Collective. (2014). *Security in-a-Box*.
57. The New York Times. (2016, February 17). *Explaining Apple's Fight With the F.B.I. - The New York Times*. https://www.nytimes.com/2016/02/18/technology/explaining-apples-fight-with-the-fbi.html
58. The Republic of Uganda. (2019). *Data Protection and Privacy Act 2019*. https://ict.go.ug/site/documents/Data-Protection-and-Privacy-Act-2019.pdf
59. UnwantedWitness. (2023). *PRIVACY SCORECARD REPORT 2023 Unwanted Witness Privacy Scorecard Report | 2023*. 1–62. https://www.apc.org/sites/default/files/privacy-scorecard-report.pdf
60. UPPC. (2010). *The Wistleblowers Protection Act*. https://media.ulii.org/media/legislation/18473/source_file/68d2d1e90ac9d490/ug-act-2010-6-publication-document.pdf
61. Wanyama, E. (2026). *CIPESA Welcomes the Annulment of Sections of Uganda's Computer Misuse Act*. https://cipesa.org/2026/03/cipesa-welcomes-the-annulment-of-sections-of-ugandas-computer-misuse-act/
62. Wodi, A. (2023). Data Privacy and Security: Fair Information Principles and Data Management Strategies in a Changing World. *SSRN Electronic Journal*. https://api.semanticscholar.org/CorpusID:265110774
63. Zinkus, M., Jois, T. M., & Green, M. (2021). Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions. *ArXiv*, *abs/2105.12613*. https://api.semanticscholar.org/CorpusID:235195749