CyberLaws (Uganda)

Introduction

- Uganda's digital transformation has led to the increasing adoption of information and communication technologies (ICTs) in government, commerce, education, and private enterprises. However, this growth has also introduced new **cyber risks**, necessitating a comprehensive **legal framework** to regulate electronic transactions, protect data privacy, and prevent cybercrime. Uganda's key national cybersecurity and data protection laws include:
  - **The Computer Misuse Act, 2011**
  - **The Electronic Transactions Act, 2011**
  - **The Data Protection and Privacy Act, 2019**
- Together, these Acts provide a **multi-layered legal regime** that governs digital behavior, enforces accountability, ensures trust in online interactions, and aligns Uganda with international standards such as the **Budapest Convention (2001)** and the **African Union Malabo Convention (2014)**.

The Computer Misuse Act (2011)

The Computer Misuse Act (2011)

- **Purpose:**

The Act provides for the safety and security of electronic transactions and information systems; prevents unlawful access, abuse, or misuse of computer systems; and ensures trustworthiness in digital environments

Key Provisions

a) Unauthorized Access and Use (Sections 12–17)

- Accessing or intercepting any program or data without authority is a criminal offence.
- Offences include hacking, unauthorized modification of data, denial-of-service attacks, unauthorized disclosure of access codes, and cyber fraud.
- Penalties: Up to 10 years imprisonment or fines; up to life imprisonment for offences involving protected computers (e.g., those used for defence, banking, or public safety).

b) Cyber Harassment and Offensive Communication (Sections 24–26)

- Criminalizes use of computers to harass, threaten, or offend others online, including cyberstalking and revenge pornography.
- Recognizes psychological and emotional harm as prosecutable offences in the digital domain.

Cont’d

c) Child Protection (Section 23)

- Prohibits child pornography, including creation, distribution, and possession of indecent images of children.

d) Electronic Fraud and Enhanced Punishments (Sections 19–20)

- Criminalizes deceptive or fraudulent use of electronic systems for personal gain.
- Offences involving critical infrastructure or national security systems attract enhanced penalties, including life imprisonment.

Cont’d

e) Investigations and Procedures (Sections 9–11, 28)

- Empowers authorities to issue Preservation Orders, Production Orders, and conduct search and seizure of electronic evidence.
- Ensures admissibility of electronic records in courts of law.

The Electronic Transactions Act (2011)

The Electronic Transactions Act (2011)

- **Purpose:**

This Act regulates electronic communications and transactions, establishes legal recognition for digital records and signatures, promotes e-Government services, and protects consumer rights in online environments.

Key Provisions

a) Legal Recognition of Electronic Records and Signatures (Sections 5–8)

- Electronic records and signatures have **the same legal validity as physical documents**.
- Ensures **admissibility of digital evidence** in legal proceedings.
- Promotes **technology neutrality**, allowing various forms of secure digital authentication.

b) e-Government Services (Sections 22–23)

- Enables **public institutions** to accept, store, and issue documents electronically.
- Supports the transition to **paperless government services**, enhancing efficiency and transparency.

Cont’d

c) Formation and Validity of e-Contracts (Sections 13–19)

- Recognizes contracts formed through data messages or automated transactions as legally binding.
- Specifies rules on time and place of dispatch and receipt of electronic communications, crucial for e-commerce and cross-border trade.

d) Consumer Protection (Sections 24–28)

- Requires suppliers to provide accurate information about goods and services offered online.
- Protects consumers against fraudulent or misleading online advertisements and ensures the right to cancel electronic transactions.

Cont’d

e) Liability of Service Providers (Sections 29–32)

- Defines safe harbor provisions for ISPs and digital platforms.
- Service providers are not liable for third-party content if they act as intermediaries and remove illegal content upon notification.

The Data Protection and Privacy Act (2019)

The Data Protection and Privacy Act (2019)

- **Purpose:**

To protect individuals' privacy and regulate the collection, processing, storage, and use of personal data in Uganda.

- The Act aligns with global data protection standards such as the EU's GDPR.

Key Provisions

a) Principles of Data Protection (Section 3)

- Every data collector, processor, or controller must:
- Be accountable to the data subject.
- Collect and process data fairly and lawfully.
- Ensure data accuracy, minimality, and relevance.
- Maintain security safeguards and respect data subject participation.

b) Institutional Framework (Sections 4–6)

- Establishes the Personal Data Protection Office (PDPO) under the National Information Technology Authority (NITA-U).
- The PDPO is responsible for monitoring compliance, handling complaints, and promoting awareness of privacy rights.

Cont’d

c) Data Collection and Processing (Sections 7–19)

- Requires informed consent before collecting or processing personal data.
- Regulates data relating to children and sensitive data (e.g., health, religion, political opinions).
- Mandates that data be collected for specific, lawful purposes and retained only as long as necessary.

d) Rights of Data Subjects (Sections 24–28)

- Individuals have the right to:
- Access personal information held about them.
- Rectify or erase inaccurate or outdated data.
- Prevent data processing for direct marketing.
- Object to automated decision-making.

Cont’d

e) Security and Cross-Border Transfers (Sections 20–23, 19)

- Data controllers must apply appropriate technical and organizational safeguards.
- Transfers of data outside Uganda are permitted only if the recipient country offers equivalent protection or with the explicit consent of the data subject.

f) Offences and Penalties (Sections 35–38)

- Criminalizes unauthorized disclosure, sale, or destruction of personal data.
- Holds corporations and individuals liable for breaches, with provisions for compensation to affected persons.

Regulation of Interception of Communications Act, 2010 (RICA)

- An Act to provide for the lawful interception of communications; to provide for the obligations of service providers to assist with such interception; to prohibit the unlawful interception of communications; and for related matters.
- Purpose: To create a lawful, supervised framework for state interception of communications for national security, public safety, and criminal investigation purposes, while simultaneously prohibiting unauthorized interception by private parties.
- RICA is perhaps the most constitutionally sensitive of Uganda's cyber laws. It authorizes the interception of private communications by the state — a power that directly engages the constitutional right to privacy under Article 27 of the Uganda Constitution

Key Provisions

- Section 5 — Warrant Requirement: Interception of communications requires a warrant issued by the Minister of Internal Affairs on the recommendation of an authorised officer. Critically, this is an executive warrant — no judicial authorisation is required.
- This is among the most criticised features of the Act, as it means the executive branch authorises its own surveillance powers without independent judicial oversight.
- Section 6 — Grounds for Interception: The authorised grounds are national security, the prevention of serious crime, and the protection of public health or safety.
- These grounds are broad and their interpretation is left largely to the executive.
- Section 7 — Obligations of Service Providers: Telecom operators, internet service providers, and other communication service providers must install and maintain technical capacity to enable interception when directed and must cooperate fully with lawfully authorised interceptions.
- This obligation extends to providing real-time access and stored communications.

Cont’d

- **Section 9 — Monitoring Centre:** The Act establishes a centralised government monitoring centre with access to communications infrastructure across Uganda. The precise operational scope of this centre has not been made public.
- **Section 10 — Confidentiality:** Intercepted communications must be treated as strictly confidential and used only for the purpose for which the warrant was issued. Disclosure to unauthorised persons is prohibited.
- **Section 17 — Prohibition on Unlawful Interception:** Any interception of communications without a valid warrant is a criminal offence punishable by up to 10 years imprisonment. This provision applies to private actors — corporations, individuals — as well as to state actors acting outside their legal authority.
- **Section 18 — Prohibition on Disclosure:** Disclosing intercepted communications without authorisation — including disclosing that a warrant has been issued — is a separate criminal offence.

HUMAN RIGHTS CONCERN

- Under RICA, interception warrants are issued by the Minister of Internal Affairs — a member of the executive branch of government — rather than by an independent court. This is a significant departure from international human rights standards on surveillance.
- The UN Special Rapporteur on Privacy and major human rights organisations including Amnesty International and Human Rights Watch, have noted that:
- Interception authorised by an executive minister lacks the independence necessary to genuinely protect against abuse. The minister is both the requester and the authoriser.
- The "national security" ground for interception is broad and susceptible to expansive interpretation. There is no requirement to demonstrate that conventional investigative means have been tried and failed.
- Civil society organisations in Uganda, including Unwanted Witness Uganda and CIPESA, have documented cases where interception powers have been used against political opponents, journalists, and human rights defenders.

Uganda Communications Act, 2013 (UCA)

- An Act to establish the Uganda Communications Commission; to provide for licensing of communication services; to regulate communications and related activities in Uganda; and for related matters.
- Purpose: To create an independent regulatory authority — the Uganda Communications Commission (UCC) — to license, monitor, and regulate all forms of communication services, ensure quality and access, manage the radio frequency spectrum, and protect consumer interests.
- The Uganda Communications Act establishes the regulatory architecture for all communications in Uganda, including telecommunications, broadcasting, and internet services. The UCC is its primary enforcement body.

Key Provisions

Section 5 — Establishment of the UCC: The Uganda Communications Commission is established as an independent body corporate with the power to regulate all communications services in Uganda. Its mandate covers telecommunications, internet services, broadcasting, and postal services.

Section 22 — Licensing Regime: All providers of communication services — telecom operators, internet service providers, broadcasting stations — must hold UCC licences. Operating without a licence is a criminal offence.

Section 26 — Consumer Protection: Service providers must maintain minimum service quality standards. The UCC may investigate consumer complaints, mediate disputes, and issue directions to providers to address systemic service failures.

Cont’d

Section 27 — Universal Access: The UCA includes obligations to expand communications services to underserved and rural areas of Uganda — recognising that universal access to communications is a public interest objective.

Section 31 — Spectrum Management: The UCC manages and assigns radio frequency spectrum to telecommunications operators and broadcasters, preventing interference and ensuring efficient use of this public resource.

Section 83 — Content Regulation: The UCC may regulate content on broadcasting platforms and electronic communications services. This is a broad power that has been the subject of controversy regarding its application to online platforms and social media content.

Section 85 — Powers to Block: The UCC and the government have powers to suspend or restrict communications services in specified circumstances. These provisions were controversially invoked during the 2021 general election period to block social media platforms, and subsequently to block internet access entirely.

Q&A