ORTUS ADVOCATES

THE LEGAL FRAMEWORK GOVERNING CYBERCRIME

Silver Kayondo

Partner

ORTUS ADVOCATES

Introduction

Despite simplifying daily life, technological advancements have resulted into grave violations of property rights, privacy and human life.

Increased frequency of cybercrimes, piracy, hacking and improper electronic data usage has led to enactment of laws to protect various rights and liberties with the international law and human rights framework.

Legal Framework for Cybercrime in Uganda

- The Computer Misuse Act, 2011
- The Electronic Transactions Act, 2011
- The Electronic Signature's Act, 2011
- The Uganda Communication's Act, 2013 (as amended) and Regulations thereunder (2019)
- The Anti-Pornography Act, 2014
- The Regulation of Interception of Communications' Act 2010 and Regulations thereunder (2023)
- The Anti-terrorism Act, 2002
- The National Information Technology Authority, Uganda Act, 2009 and Regulations thereunder

UGANDAN ACT/ REGULATION	PROVISION	COMMENTS
Computer Misuse Act, 2011 (CMA)	Sections 9,12,15,23,24,25 & 26	The legislation criminalizes unauthorized computer program access, child pornography, cyber harassment, and stalking, while also implementing preventive measures that violate certain human rights.
Uganda Communications Act, 2015 (UCA)	Sections 4 & 5	While it strengthens Uganda Communications Commission's role in monitoring and regulating communications for public safety, it lacks specific focus on cybercrime.
The National Information Technology Authority, Uganda Act, 2009 (NITA)	Sections 5, 19, 20 & 38	Provides for the functions of the authority whose scope is not defined. Thus these far reaching powers of entry and inspections can lead to violation of privacy as individuals cannot foresee the kind of information that is relevant to NITA-U

UGANDAN ACT/ REGULATION	PROVISION	COMMENTS
Electronic Signature Act, 2011 (ESA)	Sections 13,14,88,91	Need for NITA-U to establish the central e-signatures registry for authenticity and authentication purposes. No admission of e-signs in will, codicils and financial withdrawals, URSB still requiring wet signatures.
Regulations of Interception of Communications Act, 2010 (RICA)	Sections 3, 5 (c-d),7,8,9,10,11,15, 19(4),19(5).	Complexities in sim-card registration for corporations and partnerships need to be ironed out.
The Anti-Pornography Act, 2014.	Sections 11,13(2),14(1) & 17	Enforcement is challenging, given that most pornography sites are internet-based.

UGANDAN ACT/ REGULATION	PROVISION	COMMENTS
Electronic Transaction Act, 2011. (ETA)	Sections 19, 29,30,32	The legislation criminalizes electronic fraud, imposing penalties and protect service providers from being held accountable for the digital material they merely facilitate access to.
Data Protection and Privacy Act, 2019.	Sections 35,36,37.	The legislation protects the privacy of people's personal data as it makes it an offence to disclose, alter, delete or even sell personal data.
The National Information Technology Authority-Uganda (E-Government) Regulations, 2015.	Regulation 15(2)	This law estops public bodies from disclosing personal information without the respective party's consent..

The Computer Misuse Act, 2011

It addresses various offences, including unauthorized access, interception, cyber harassment, and offensive communication

Section 12(1) aims to combat hacking which involves unauthorized access to computer systems, networks, or data with malicious intent. **Uganda v. Guster Nsubuga & Others**

Sections 23-26 outline clear definitions and penalties for offences like child pornography, cyber harassment, offensive communication and cyber stalking.

Uganda vs. Dr. Stella Nyanzi

Electronic Transactions Act, 2011

It aims to ensure integrity and security in electronic communications and transactions.

Section 19 criminalizes electronic fraud, imposing penalties of up to 360 currency points or imprisonment not exceeding ten years or both for deceitful activities aimed at unlawfully gaining financial advantages through digital means. **Uganda vs. Mutambira John Tiryarenga**

It combats identity theft and fraud by protecting sensitive information and shields internet service providers from liability concerning third party as delineated in **section 29** ensuring that providers are not held accountable for the digital material they merely facilitate access to.

Anti-Pornography Act

The Act aims to curb the spread of pornography by imposing severe penalties for its production, distribution, and consumption, thereby combatting cyber stalking and harassment, while also safeguarding societal morals and minor's welfare.

Section 13 prohibits activities like producing, distributing, broadcasting or facilitating access to pornography with violations leading to decade long imprisonment.

Furthermore, **Section 14(1)** intensifies penalties for offenses involving child pornography, aligning legal consequences with the gravity of the crime and should be read together with S.23 CMA that provides for the offence of child pornography. **Uganda v. Emin Baro.**

Regulation of Interception of Communications Act, 2010

- It introduces significant tensions between national security imperatives and individual privacy rights guaranteed in Article 27 of the Constitution.
- **Section 3** of the Act, the Minister of security is obliged to establish and maintain a communication interception Monitoring Centre to capture such acts of terrorism.
- Section 7, Section 19 (5), Section 19 (4), Section 8, Section 10, Section 11, and section 15 are related to the interception of communications, obligations on telecommunications and internet service providers, decryption of communications, data retention, and transparency requirements. This tackles ransomware attacks, a type of malware that encrypts a victim's files, with the attacker then demanding a ransom from the victim to restore access to the data upon payment.
- **Section 9** provides that telecommunications service providers also have a duty to ensure that subscribers register their SIM-cards and provide service providers with comprehensive information about e.g. their identity and address.

Anti-terrorism Act, 2022

- The Act is aimed at combatting terrorism through surveillance and interception, specifically identifies hacking as a potential terrorist act under certain conditions. These conditions include threats to influence the government, intimidate the public, and advance political, religious or ideological causes. The Act allows targeted interception in terrorism-related investigations, but raises concerns about potential rights infringements and the need for stronger judicial oversight and civil liberties protections.

- The Act's broad provisions may criminalize legitimate behavior, including human rights like freedom of expression, due to their overly broad language.

The Uganda Communications Act, 2013

- **Section 4** of the Uganda Communications Act of 2013 empowers the Uganda Communications Commission (UCC) to act independently and with significant regulatory authority in section, including the directive power during states of emergency, as seen during the 2011 and 2016 social media access restrictions.

- Furthermore, the UCC's functions allow for extensive supervision and control of communications under UCA, potentially infringing on privacy and freedom of expression. A good example is **section 5(u)** that has been used to establish social media monitoring centers and interception centers under RICA for communication surveillance, such as internet communications.

National Payments Systems Act, 2020.

- Section 4 of the Act provides that the central bank in Uganda shall regulate and supervise payment systems, issue licenses, and administer the Act.

- The Central Bank shall also consider license applications and monitors cross-border payments which monitoring can help detect any suspicious/fraudulent transactions.

- Part IV of the Act outlines regulatory measures that are essential for mitigating the risks of cybercrime within the electronic money sector.

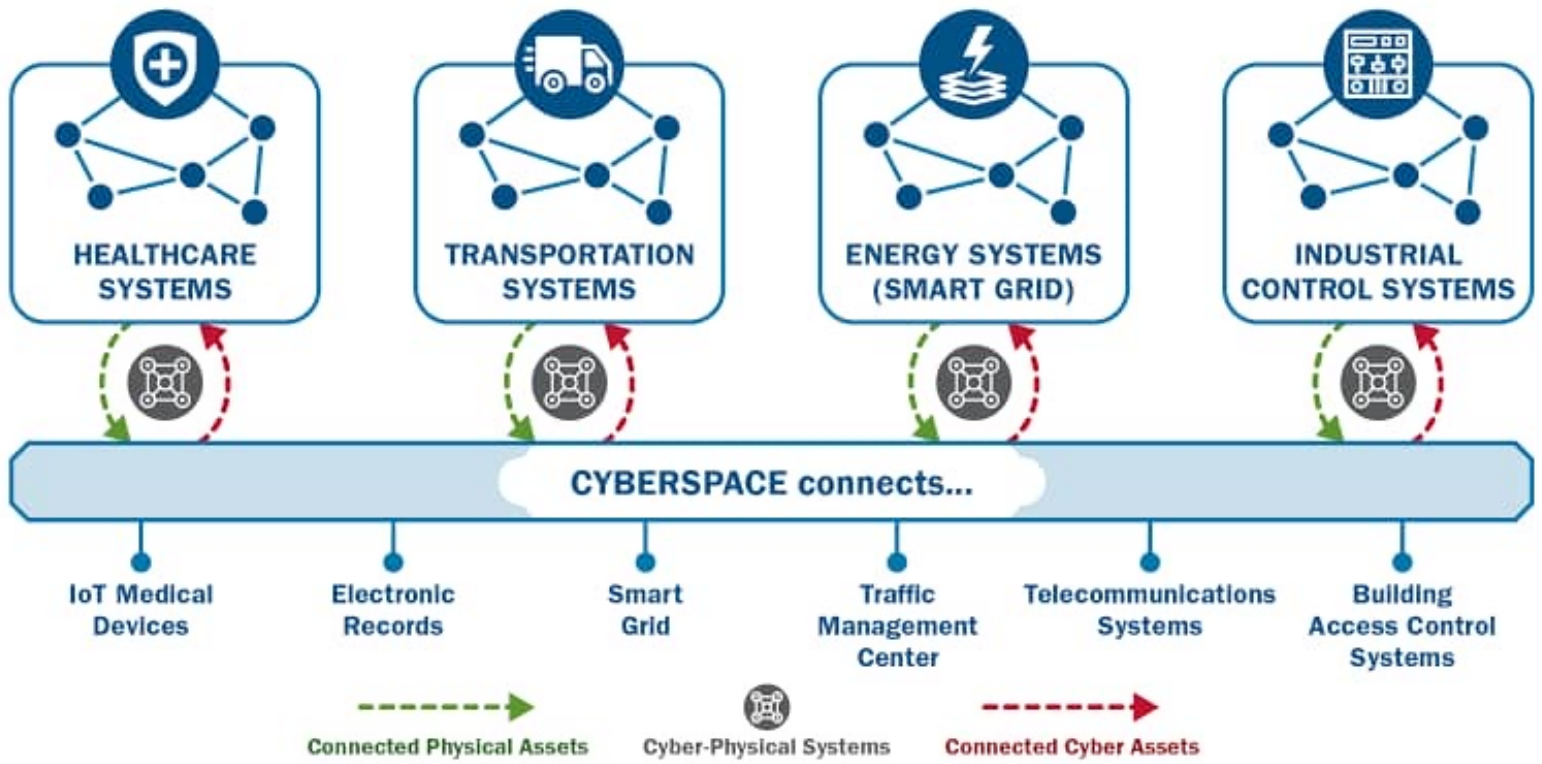
- Section 47 requires electronic money issuers and payment service providers to collect and submit customer information helps in identifying individuals engaging in financial transactions. This is essential for tracking and investigating cybercriminals who may exploit electronic payment systems for illicit activities.

Anti-Money Laundering Act, 2013.

- By mandating that accounts be maintained in the true name of the account holder and prohibiting anonymous or fictitious accounts, **section6(1)** helps prevent identity theft and fraud as cybercriminals often exploit anonymity to create fake accounts for malicious purposes. Ensuring accurate identification reduces the risk of such fraudulent activities.
- The requirement to verify the identity of clients using reliable, independent sources makes it difficult for cybercriminals to use stolen identities or fabricated details to open accounts or conduct transactions.
- Prohibiting the disclosure of suspicious activity reports (SARs) to customers or any unauthorized persons under **section 9(6)** protects the integrity of investigations and prevents tipping off criminals. This is crucial in cybercrime cases where premature disclosure could lead to data destruction, evidence tampering, tip off, or flight of suspects.
- The requirement to report suspicious transactions, regardless of their value, ensures that low-value cybercriminal activities are detected, as they often use "smurfing" techniques to split large sums.

Cyber-physical Convergence

Cybercrime encompasses not just data and financial theft but also physical impacts, including physical risks associated with daily operations. Criminals sometimes use cyber methods to enhance existing operations, blurring the lines between traditional crime and cybercrime due to increasing digitalization and globalization.



ORTUS ADVOCATES

Gap Analysis

The Anti-Terrorism Act (ATA) does not clearly define what constitutes terrorism promotion, potentially leading to arbitrary application and difficulty for media and individuals in identifying which material is considered terrorism-promoting.

The country's current legal framework falls short in areas like cross-border data protection, cybercrime cooperation, and stringent privacy regulations as most of the laws enacted in one way or another infringe of the right to privacy and freedom of expression.

The rapid advancements in technology and the internet pose significant challenges to the effectiveness of laws, as they often exceed the specific provisions of the law, leading to potential legal ambiguities.

The ETA, while effective in promoting a secure e-commerce environment, has a narrow focus on transactions, suggesting potential for improvement in incorporating a wider range of cybercrime deterrents..

Gap Analysis Continuation

•Under the NITA-U, information technology surveys cover both public and private sectors, making it difficult for individuals to predict what information might be of interest to the NITA-U.

•Section 8 of the Regulation of Interception of Communications Act, 2010 mandates service providers to install equipment for interception of communications, with failure to do so resulting in a prison sentence of up to five years.

•No clear parameters for live political reporting via OTT platforms in UCC Guidelines & Regs and Electoral Commission Act and Regs

•No clear guidelines on online drugs advertisements and promotion under National Drug Authority's purview

•No clear framework for emerging technologies such as AI, VR/AR, Satellite and drones/UAVs

A lawyer and his drones

ORTUS ADVOCATES

Gap Analysis Continuation

- Under CMA, police officers have extensive search and seizure powers, which, combined with a low threshold for evidence, pose a threat to privacy and freedom of expression. They also have broad access to people's computer data, thereby posing a risk of privacy violations.
- Section 19(5) of the authorization allows for the interception of various forms of communication, including letters, telephone calls, emails, meetings, movements, activities, electronic surveillance, access to bank accounts, and searching premises. Additionally, the authorized officer has the right to detain, copy, take photographs, and perform other necessary actions. Consequently, such surveillance practices can impede freedom of expression and right to privacy of the citizens.
- VPNs can hinder law enforcement's ability to track and monitor illegal online activities, creating a regulatory gap in Ugandan cybercrime laws which often rely on IP addresses. Current laws lack specific provisions for the use and regulation of VPNs, leaving providers without registration or data retention requirements, thereby highlighting the need for improved enforcement of digital footprints in cybercrime.

Recommendations continuation

Section 7 of the Anti-Terrorism Act allows for the death penalty for minimal infractions and legitimate human rights violations. The UNHRC emphasizes the importance of respecting the principle of proportionality in both the law framed by restrictions and the administrative and judicial authorities in applying the law. The Act should clearly differentiate between different offense categories and penalties to ensure proportionate and necessary sanctions for the Act's legitimate interests.

The above proposals calls for the creation of independent oversight bodies to address actions that could potentially harm fundamental rights and freedoms, and for ministers' powers to be limited to a system of impartial judges or oversight commissions.

Given that VPN services are cross-border, international collaboration is crucial. Uganda should collaborate with other nations to create protocols and agreements for information exchange and coordinated efforts against cybercriminals using VPN.

More gaps

Section 7 of the Anti-Terrorism Act allows for the death penalty for minimal infractions and legitimate human rights violations. The UNHRC emphasizes the importance of respecting the principle of proportionality in both the law framed by restrictions and the administrative and judicial authorities in applying the law. The Act should clearly differentiate between different offense categories and penalties to ensure proportionate and necessary sanctions for the Act's legitimate interests.

The above proposals calls for the creation of independent oversight bodies to address actions that could potentially harm fundamental rights and freedoms, and for ministers' powers to be limited to a system of impartial judges or oversight commissions.

Given that VPN services are cross-border, international collaboration is crucial. Uganda should collaborate with other nations to create protocols and agreements for information exchange and coordinated efforts against cybercriminals using VPN.

International landscape impacting Ugandan laws

- Cyber sanctions (US, UK, EU regimes)
- Cloud & data center facilities (onshore & offshore)
- Look at cross-border. Mutual Legal Assistance Agreements
- IP addresses registry
- Domain names registry- Cyber squatting
- Cyber criminal registries?
- Cyber espionage and national security

Cyber warfare

ORTUS ADVOCATES

Emerging aspects to consider

- Theft of trade secrets and IP. Are our IP laws adequate?
- Cyber warfare- spill overs from global conflicts e.g Ukraine
- Voice, image, text & video manipulation/deep fakes
- Forensics & laboratory accreditation
- Electronic searches & seizures
- Expert witnesses and expert evidence
- Evidence & exhibit handing.
- Virtual registers & Cyber crime scenes
- Cyber investigations & online trials

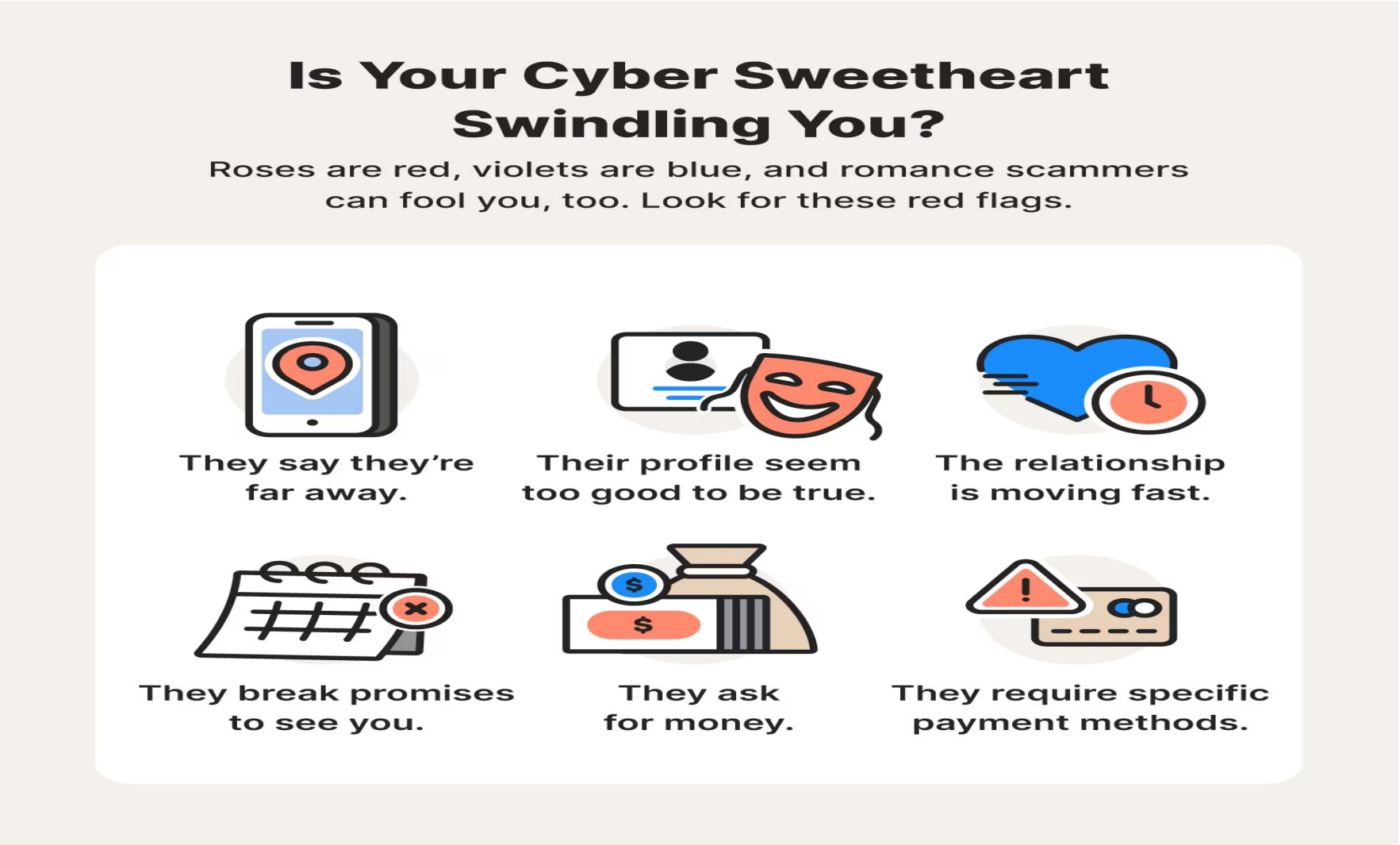
Back home- an eye to the future

- Tier 4 Money Lenders Act. Digital Credit Provider Guidelines, 2024
- Police Act- ripe for amendment?
- Evidence Act- how will it cope with AI, VR and simulated evidence?
- UPDF Act- a stronger case for national security exceptions?
- The Constitution (Integration of ICT into the Adjudication. Process for Courts of Judicature) (Practice) Directions, 2019 and ECCMIS- How far shall we go?
- E-tax/EFRIS- A new round of fraud? Uganda vs Guster Nsubuga & 3 Others (2012)
- Utilities Court- growing Computer misuse trends. Consider decentralization of the Court and UCC's prosecutorial capacity?
- Time for Advocates Social Media Guidelines?

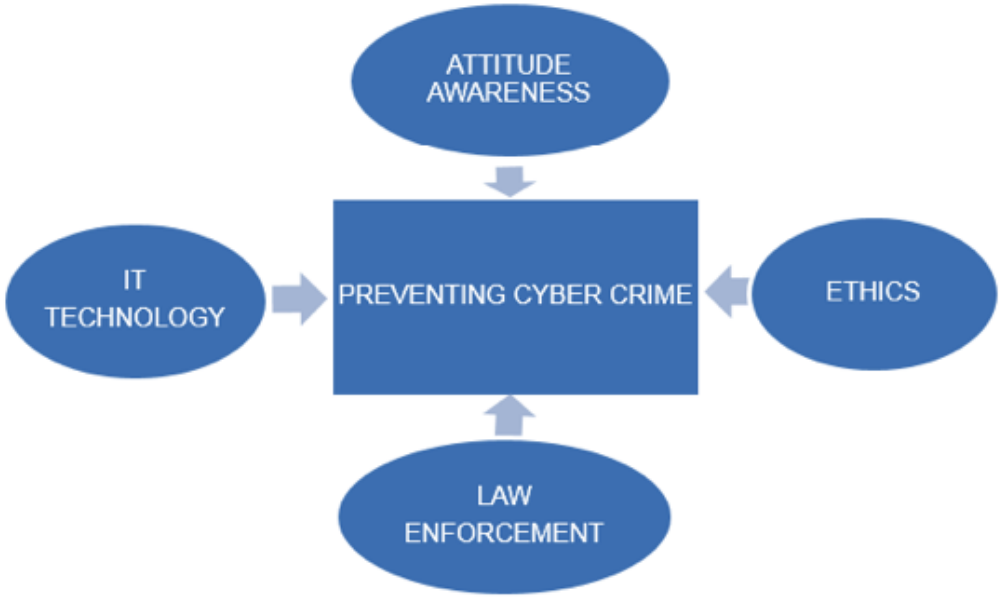
Practical challenges

- Limited capacity of police, especially upcountry
- Conflict of interest (employees)
- Lack of investigative and prosecutorial cooperation (insider fraud)
- Delays- Courts (real-time frauds)
- Lack of a depositor protection/insurance fund for cyber frauds (consumer protection)

The “romantic” side of cyber crime



ORTUS ADVOCATES



ORTUS ADVOCATES

Conclusion

Uganda's cyber law framework, including the Computer Misuse Act and Electronic Transactions Act, is effective in addressing cyber-related offenses. However, challenges like rapid technological advancements, enforcement difficulties, and public awareness need to be addressed.

Strengthening the framework requires regular updates, enhanced enforcement capabilities, and increased user education. Despite Uganda's progress, ongoing adaptation and resource allocation are crucial for effective cybercrime prevention.

ORTUS ADVOCATES

Thank you

“What is the argument on the other side? Only this, that no case has been found in which it has been done before. That argument does not appeal to me in the least. If we never do anything which has not been done before, we shall never get anywhere. The law will stand still whilst the rest of the world goes on; and that will be bad for both.” Lord Denning MR (as he then was) Packer v Packer (1953) 2 ALL ER 127

Email: skayondo@ortusadvocates.com

Tel: +256779334187

ORTUS ADVOCATES