Lawpoint Uganda

Making the Law Easy and Accessible

DPO PRIVACY CENTRE EAST AFRICA

UGANDA'S DATA PRIVACY LAWS: SAFEGUARDS AND FLAWS IN THE DIGITAL AGE

BY:
BYARUHANGA JOSHUA MORRIS

ABSTRACT

With the digital economy expanding rapidly, personal data is now crucial, necessitating the protection of citizens' privacy rights. This right is fundamental as per Article 27 of the 1995 Constitution as Amended. However, with the digital landscape evolving, we must assess if the "Digital Shields"—the Data Protection Laws—can withstand the challenges posed by Artificial Intelligence, Biometric Tech, Block-chain, and Fin-tech. This article evaluates Uganda's Data Protection Laws against past data breaches, compares them with Kenya's laws, and offers recommendations for the digital economy.

The Digital Shield : The Data & Privacy Act Cap 97

The Data Protection and Privacy Act Cap 97 was enacted in 2019, and its regulations took effect in 2021. Regarded as Uganda's digital shield, these provide a framework for personal data collection, processing, and storage. Uganda's laws are based on principles of transparency, accountability, fair processing, purpose limitation, data minimization, data quality, and security safeguards.

The **Personal Data Protection Office (Personal Data Protection Office)** acts as the guardian of these principles, tasked with investigating infringements and maintaining a data protection register. The Act also establishes criminal digital offenses to penalise the misuse of personal information, such as unlawfully obtaining, disclosing, or altering personal data. Beyond individual liability, **corporations can be held criminally liable**[2] if their officers knowingly authorize or permit these contraventions[3].

The First Cracks of the Data Protection and Privacy Act Cap 97

Despite noble intent, the Act has critical flaws that undermine its effectiveness:

1. **Ambiguous Consent:** The Act lacks clear criteria for informed consent and no provision for withdrawal.
2. **Inadequate cross-border rules:** Section 19 requires measures for data transfers but lacks strict mechanisms.
3. **Uncertain retroactivity:** The Act is silent on pre-2019 data, creating a legal grey area.
4. **Independence of the Personal Data Protection Office:** The office is under NITA-U, compromising its independence.
5. **Quasi-Judicial Limitation:** The office is investigative, not adjudicative, relying on courts for solutions.
6. **Weak Penalties:** Sanctions are mild; maximum fine for corporations is 4.8 million UGX.

An Analysis of Recent Data Protection Decisions

a) The Nano Loans Case (July 2024) : Ronald Mugulusi was convicted for sharing a borrower's personal data on TikTok. While it proved the law is enforceable, the penalty of approximately 300,000 UGX (approx. $80 USD) was considered too weak to be effective.

b) Ssekamwa Frank & 3 ors v Google LLC: The Personal Data Protection Office ruled against Google LLC after activists complained about unlawful data processing. Google argued it was not subject to Ugandan law as it was not domiciled there, but the Personal Data Protection Office asserted that any entity processing data of Ugandan citizens must follow Ugandan laws, regardless of location.

The Fin-tech Industry vis a vis Data breaches

The Fin-tech industry is rapidly growing in Uganda and Africa, mainly in mobile and online banking. Reports show a 32% compound annual growth rate by 2030, highlighting the need for strong laws to protect the industry. Furthermore, the Bank of Uganda's 2024 Financial Stability Report indicates a 38% rise in cyber threats that year. Notable breaches include:

Pegasus Technologies Hack (October 2020): This Incident surrounded a security breach at Pegasus Technologies , a consumer finance aggregator ,compromised of bank to wallet transfers . Around 2,000 mobile SIM cards were used by hackers to compromise bank-to-mobile wallet transfers, resulting in an estimated $3.2 million USD stolen.

Diamond Trust Bank (DTB) Breach (December 2023): DTB Kenya and its subsidiary in Uganda were fined by the Kenyan Data Commissioner for mishandling customer data in a cross-border banking error which involved improper data sharing affecting personal information in Fin-tech operations spanning both countries.

Bank of Uganda Cyber Attack (November 2024): Hackers known as "Waste" stole approximately 62 billion Ugandan shillings ($16.5–17 million). While the Bank downplayed the amount, investigations into insider collusion are ongoing. The Act remains silent on the specific liabilities of third-party aggregators who sit between banks and telecommunication companies.

Biometric, Block chain, and AI Technology

Bio-metrics: The National digital ID system (Ndaga Muntu) managed by NIRA collects fingerprints and facial images for over 26 million citizens. A September 2024 BBC investigation alleged that personal data from the register was accessed by a sex-trafficking ring. The Act lacks specific rules for large-scale biometric systems rolled out before its enactment.

Block-chain Technology is a decentralized , immutable digital ledger that records transactions in a transparent and secured manner across a distributed network of computers. A good example of Block chain Tech is crypto currency, while the High Court ruled cryptocurrency as an illegal payment instrument , the sector still remains a "legal gray area" prone to data breaches as seen in the **2019 Dunamiscoin Scam** , where 4,000 investors lost $2.8 million highlighting a lack of oversight and consumer protection . Despite the lack of legal recognition of cryptocurrencies, VASPs (Virtual Assets Service Providers) are still considered and recognized by the Financial Intelligence Authority therefore highlighting a need for our Data Protection Laws need to recognize block-chain technology11.

Artificial Intelligence is defined as a technology involving algorithmic decision-making, generative models, and automated systems that has the potential to transform sectors such as health, education, and business. In the Ugandan public sector, AI is specifically valued for its ability to turn months of manual work into seconds of automated insight. While 97.9% of Ugandan Ministries, Departments, and Agencies (MDAs) have functional computers and websites, only 21% have taken concrete steps toward Fourth Industrial Revolution (4IR) integration. Of that specific group, only 29% have integrated AI into their operations.

Globally, **13% of organizations** reported breaches specifically involving their AI models or applications between 2024 and 2025. In Uganda, **59% of MDAs** reported experiencing cyber incidents in the prior year. Therefore highlighting a great need for our Data Protection Laws to provide for AI.

Regional Benchmarking: The Data Protection and Privacy Act Cap 97 in comparison with the Kenyan Data Protection Act 2019

While sharing a common foundation, the two frameworks diverge:

Independence: The Kenyan Data Commissioner is an **independent body corporate**, whereas the Ugandan Personal Data Protection Office is linked to NITA-U.

Enforcement: The Kenyan Commissioner can impose **direct administrative fines** , while Uganda's Personal Data Protection Office relies on court-prosecuted fines this can also be highlighted by the **Kennedy Omondi Ochieng v Fingrow Capital Limited ODPC Complaint No. 1966 of 2024**, were the Kenyan Data Protection Commissioner found the respondent liable for unlawfully disclosing financial data and **directly ordered the respondent to pay the complainant KES 200,000 in compensation.** In contrast, Uganda's Personal Data Protection Office (PDPO) **lacks the power to award compensatory relief or issue direct administrative fines** For instance, in the landmark July 2025 ruling against **Google LLC**, the PDPO noted it could not offer compensation to the digital activists, as such relief must be pursued separately through the **court system.**

Data Portability: The right to data portability is a data protection principle that empowers individuals to have greater control over their personal information by allowing them to move it between different service providers. This right is granted in Kenya but is not explicitly listed in Uganda.

Recommendations and Way Forward

1. **Secure Institutional Independence** of the Personal Data Protection Office from NITA-U.
2. Amend laws to grant the Personal Data Protection Office **quasi-judicial powers** and the ability to issue administrative fines.
3. Bridge the knowledge gap through **digital literacy** collaborations with civil society.
4. Apply **stringent** measures to non-compliant companies, including Big Tech.
5. Proactively **amend** the Act by 2027 to include emerging technologies and the right to portability
6. Encourage ongoing dialogue between government and the private sector.

Conclusion

Uganda's journey toward robust data protection is ongoing. While the Act established a "digital shield," the "weak bite" of recent convictions shows the framework lacks the "strong arm" needed to deter bad actors. Uganda must look to regional blueprints, like Kenya's model, to bridge its own legislative and institutional gaps.

"Data privacy is not merely a technical concern; it is fundamentally a human rights issue. It is about protecting our autonomy, dignity, and freedom in the digital realm."

BIBLOGRAPHY

Cases cited

a. Silver Kayondo v Bank of Uganda Miscelleneous Cause No. 109 of 2022
b. Ssekamwa Frank & 4 ors v Google Compilant 08 /11/24/6683
c. Kennedy Omondi Ochieng v Fingrow Capital Limited ODPC Complaint No. 1966 of 2024

Articles cited

d) Kizito, P. (2025, December 3). DTB fined Sh500,000 for data privacy breach. Capital Business.https://www.capitalfm.co.ke/business/2025/12/dtb-fined-sh500000-for-data-privacy breach/#:~:text=The%20ODPC%20determined%20that%20DTB,Kenya%20-finance%2C%20ODPC%2C%20privacy%20violation

e) Is crypto legal in Uganda? Regulations & compliance in 2025. (n.d.). https://www.lightspark.com/knowledge/is-crypto-legal-in uganda#:~:-text=Quick%20Answer,it%2C%20leaving%20consumers%20without%20protection.

f) Uganda confirms hack of central bank accounts, official downplays extent of loss | Reuters. (n.d.). https://www.reuters.com/world/africa/hackers-steal-17-mln-uganda-central-bank-state-paper-2024-11-28/

g) Macdonald, A. (2025, September 22). Uganda to tighten biometric ID database security after data breach claims. Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/202509/uganda-to-tighten-biometric-id-database-security-after-data-breach-claims

h) Ugandans lose SHS60B in football ponzi scheme | Monitor. (n.d.b).https://www.monitor.-co.ug/uganda/news/national/ugandans-lose-shs60b-in-football-ponzi-scheme-3985224

i) https://www.monitor.co.ug/uganda/business/technology/uganda-s-data-protection-law-takes-effect-first-ever-conviction-5129964

j) How AI Is Helping Government Companies in Uganda Cut Costs and Improve Efficiency, https://www.nucamp.co/blog/coding-bootcamp-uganda-uga-government-how-ai-is-helping-government-companies-in-uganda-cut-costs-and-improve-efficiency

Websites

Personal Data Protection Office | Personal Data Protection Office - UG. (n.d.). https://Personal Data Protection Office.go.ug/about-us

Statutes Cited

k) The Data Protection and Privacy Act Cap 97

l) The Kenyan Data Protection Act (No.24 of 2019)