

Rights Trends, Regulatory Gaps and Policy Responses

The image displays a complex financial data dashboard titled "MAIN HUB for STATISTICS & DATA". The interface is divided into several functional areas:

- INDEX WATCH:** A sidebar on the left with a "MOVE QUOTES" button and a list of market indices (e.g., S&P 500, NASDAQ, DOW JONES) with their respective values and percentage changes.
- PORTFOLIOS:** A section for tracking investment portfolios, showing names like "PORTFOLIO 1" and "PORTFOLIO 2" with their performance metrics.
- Internal Stock Process Listings:** A central table listing various stocks with columns for stock symbols (e.g., HUV, IVO, IVD, TPP, LDR), numerical values, and percentage changes. It includes a "TRADE" button.
- ANALYTICAL TOOLS:** A section for data analysis, featuring a "SERIES" button and a list of data series (e.g., HUV, IVO, IVD, TPP, LDR) with their corresponding values and percentage changes.
- Ultra-High Stock Market List:** A section displaying a list of high-value stocks, including their names (e.g., HUV, IVO, IVD, TPP, LDR) and their market values.
- Advanced Demographic Info:** A section showing demographic data, including a bar chart and a pie chart, with a "SERIES" button.

The interface is designed for professional use, with a clean, modern aesthetic and a focus on data visualization and analysis. A small text box on the right side of the screen reads: "The W.B. & A. is a... (text is partially obscured)".



Introduction

Uganda has made digital transformation a central pillar of its socio-economic development. Under its Digital Transformation Roadmap, the government targets 90% household internet connectivity, 90% broadband coverage by geography, and 90% of citizens accessing e-services online by 2040.¹

This progress is significant, but so too is the governance gap behind it. Uganda's digital economy is expanding faster than the legal, regulatory and institutional frameworks needed to govern it. That gap manifests in four key ways. First, the digital economy increasingly depends on personal and biometric data, yet important questions remain about how businesses collect, use, store and dispose of it.

Secondly, recurring state-ordered internet disruptions undermine the stable environment online commerce and financial services depend on. Third, Artificial Intelligence (AI), blockchain and robotics are reshaping the labour market, creating opportunities while disrupting existing work faster than labour regulation can respond. Finally, digital technologies, particularly AI, are evolving faster than regulatory and institutional capacity, creating risks of surveillance, opaque decision-making and digital exclusion. If these gaps are not addressed, they could undermine the transformation Uganda is pursuing.

Drawing on a 2025 [survey](#), two [commentaries](#) and a policy submission - all by the Collaboration on International ICT Policy for East and Southern Africa (CIPEA) - this brief examines emerging digital businesses, assesses the adequacy of Uganda's legal and institutional framework, analyses business data practices, explores the changing world of work, and evaluates the impact of internet shutdowns, before presenting recommendations for a digital economy that advances innovation while protecting digital rights.

¹ Ministry of ICT and National Guidance, Digital Transformation Roadmap, FY2023/24-2027/28 (2023), <https://ict.go.ug/site/documents/Digital%20Transformation%20Roadmap.pdf>

1. A Fast-Growing Digital Economy

Uganda's digital economy is expanding rapidly across finance, transport, agriculture, commerce and healthcare, creating opportunities for financial inclusion, employment and service delivery. This growth is driven by rising digital adoption, expanding connectivity and innovation by both established firms and start-ups.

In finance, Emata Uganda and Quest Digital Finance are scaling digital credit for cooperatives, smallholder farmers and Small and Medium-Sized Enterprises (SMEs), while the Uganda Development Bank's AgriConnect targets 1,000 smallholder farmers in West Nile and Northern Uganda. Mobile money and agent banking have grown significantly, with agent banking transactions reaching Uganda Shillings (UGX) 29.4 trillion by June 2025, up 76% year-on-year, with agents on the shared platform growing 49.1% to 22,793 over the same period, according to the Bank of Uganda.²

Ride-hailing platforms including Uber, Bolt and SafeBoda continue to expand, though concentrated in urban areas. The International Labour Organisation (ILO) estimates SafeBoda alone has registered roughly 28,000 riders and 3,000 drivers.³ Digital platforms such as TikTok are creating new income opportunities for youth through content creation and marketing, while agricultural apps like Market Garden App and AgroMarket Day connect farmers, particularly women, to markets and advisory services. E-commerce platforms Jiji and Jumia continue to grow, with Jiji sellers reportedly earning an average of USD 150 weekly, and digital health providers such as Rocket Health are broadening access to care through telemedicine.

2. Regulatory Framework Struggling to Keep Pace

The constitutional foundation for privacy in Uganda is article 27 of the 1995 Constitution, which protects against unlawful search, entry and interference with a person's home, correspondence or communications.⁴ As digital businesses collect, process and store growing volumes of personal and biometric data, this foundation is increasingly tested, raising important questions about whether existing safeguards remain fit for purpose.

The Data Protection and Privacy Act, 2019, and its 2021 Regulations, form the core of the framework that governs how public and private entities collect, process, store and share personal data. These are supplemented by guidance notices from the Personal Data Protection Office (PDPO).⁵ For digital lending specifically, the Tier 4 Microfinance Institutions and Money Lenders Digital Lending Guidelines, 2024, require providers to safeguard customer information, obtain explicit consent before sharing it, and refrain from mining contact lists or messages for debt recovery.⁶ Institutionally, the Personal Data Protection Office (PDPO) is the principal oversight body for data protection, and since 2023 the PDPO has required organisations to submit standardised annual compliance reports.

The Computer Misuse Act, 2011, criminalises unauthorised access to and interference with data and empowers courts to preserve and compel production of evidence, though its effectiveness depends heavily on consistent enforcement.⁷ By contrast, the Regulation of Interception of Communications Act, 2010 grants security agencies broad interception powers on national security grounds and requires telecoms to retain customer and call metadata for at least six months, a blanket requirement that is difficult to balance with the privacy protections elsewhere in the country's legal framework.⁸

This domestic framework draws on international instruments Uganda has ratified, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples' Rights. Accordingly, Uganda's legal framework provides many of the core elements a rights-respecting digital economy needs. As the sections below show, the principal challenge lies not in the absence of laws, but in their implementation, enforcement, and adaptation to fast-evolving technology.

² "Who is Pebuu: The Ugandan Company Quietly Powering Africa's Largest Agent Banking Networks," CEO East Africa, 4 March 2026, citing Bank of Uganda data, <https://www.ceo.co.ug/who-is-pebue-the-ugandan-company-quietly-powering-africa's-largest-agent-banking-networks/>.

³ CIPESA, *The Future of Work in Uganda: Challenges and Prospects in the Context of the Digital Economy* (2025), p. 3, citing International Labour Organization, *Digital Labour Platforms in Uganda* (2024), https://cipesa.org/download/Future_of_work_in_Uganda_Challenges_and_Prospects_in_the_Context_of_the_Digital_Economy.pdf.

⁴ Constitution of the Republic of Uganda, 1995, Article 27.

⁵ Data Protection and Privacy Act, 2019 (Act 9 of 2019), <https://ulii.org/akn/ug/act/2019/9/eng@2019-05-03/source>.

⁶ Uganda Microfinance Regulatory Authority, *Digital Lending Guidelines for Tier 4 Microfinance Institutions and Money Lenders* (January 2024), <https://umra.go.ug/wp-content/uploads/2024/03/DIGITAL-LENDING-GUIDE-LINES-FOR-UMRA-2024.pdf>.

⁷ Computer Misuse Act, 2011 (Act 2 of 2011), <https://ulii.org/akn/ug/act/2011/2/eng@2011-02-14/source>.

⁸ Regulation of Interception of Communications Act, 2010 (Act 18 of 2010), <https://ulii.org/akn/ug/act/2010/18/eng@2010-09-03>.

3. Progress and Persistent Gaps in Business Practices

3.1 Business Data Practices

Businesses are collecting an increasingly wide range of personal and biometric data. Fingerprints are widely used for access control, banking, employee attendance and SIM registration; facial recognition supports national ID verification; and iris recognition is increasingly used at border points and by some banks. The country's ongoing national ID enrolment and renewal exercise, expected to reach approximately 17.2 million Ugandans involves collection of all the above biometrics. In June 2023, the Bank of Uganda announced that 74 financial institutions, including 27 commercial banks and 34 fintech firms, had gained access to the national ID database for digital Know Your Customer (KYC) verification under the Registration of Persons Act, 2015, although implementation remains gradual.⁹

Businesses cite four main reasons for their widespread data collection: legal requirements such as mandatory SIM registration; the state's own digitalisation of services like passport applications and border management; fraud prevention, with at least eight Ugandan banks, including Stanbic, Centenary, Equity, DTB, Standard Chartered, Bank of Africa, Opportunity Bank and Postbank, now running biometric-enabled mobile banking apps; and workforce management, illustrated by the case below.

Case Study: Makerere University Staff and Student Biometric Attendance System

The growing use of workplace biometrics is illustrated by Makerere University's Digital Staff Access System, launched in May 2024 and hosted by the College of Computing and Information Science, alongside an existing Student Attendance System.¹⁰ The staff system captures lecturers' thumbprints and facial features to record attendance, with voice-recognition also being explored for staff unable to use the biometric devices. The university said the system would improve accountability by letting students report lecturer absenteeism, curb staff absenteeism, and enforce standard working hours, while also generating data for teaching-load and recruitment planning.

The system nevertheless faced opposition from the Makerere University Academic Staff Association (MUASA), which argued that academic work, centred on teaching, research and community engagement, is fundamentally different from routine public service and should not be assessed primarily through fixed attendance. The dispute highlighted broader concerns about privacy, academic autonomy and the risk of reducing scholarly productivity to time spent on campus rather than academic output.

The Makerere case illustrates a broader policy dilemma facing Uganda's digital economy. Biometric technologies can improve accountability and administrative efficiency, but their deployment in workplaces raises questions about proportionality, privacy, staff autonomy and the limits of digital surveillance, questions that Uganda's current legal framework offers only limited guidance on addressing.

⁹ "74 Financial Institutions Now Access NIRA Database, Says BoU," *Daily Monitor*, 10 October 2024, <https://www.monitor.co.ug/uganda/business/markets/74-financial-institutions-now-access-nira-database-says-bou-4790144>.

¹⁰ "Makerere Staff Want Teaching Equipment, Not Biometrics – MUASA," *Daily Monitor*, 8 May 2024, <https://www.monitor.co.ug/uganda/news/national/makerere-staff-want-teaching-equipment-not-biometrics-muasa-4616532>; see also Makerere University News, "Launch of Mak Attendance Management System a Moment of Truth" (5 May 2024), <https://news.mak.ac.ug/2024/05/launch-of-mak-attendance-management-system-a-moment-of-truth/>.

3.2 Emerging Concerns

Beyond legal compliance, gaps remain in transparency, informed consent, data security and accountability. Businesses frequently collect personal and biometric data without clearly explaining what is collected, how it is processed, where it is stored or with whom it is shared. As one survey respondent put it, organisations often say only that data will be used “in accordance with our internal policies”, without further detail or access to those policies, and dense privacy notices compound the problem, leaving most customers unable to exercise their rights.

Meaningful consent is similarly undermined: it is often buried in lengthy terms that users must accept in full to access a service, a “take it or leave it” arrangement that leaves little genuine choice. Behavioural monitoring technologies, increasingly used in mobile money and digital banking to flag unusual transaction patterns for fraud detection, add another, largely invisible layer of data collection that can trigger account restrictions without users understanding why.

Data security is uneven, smaller businesses in particular often lack adequate encryption and secure storage, data minimisation is widely ignored, and third-party sharing without meaningful consent, common among advertisers and data brokers, is where the risks of misuse and unauthorised disclosure are greatest.

Case Study: SafeBoda Data Breach

The governance challenges around business data practices are illustrated by the SafeBoda data breach allegations. In 2020, SafeBoda, a ride-hailing platform operating in Uganda, Kenya and Nigeria, was accused of sharing users’ personal data with third-party applications without consent, contrary to Section 7 of the Data Protection and Privacy Act, 2019. In a complaint filed before the National ICT Authority Uganda (NITA-U), Obedgiu Sammy alleged that SafeBoda had integrated a Software Development Kit capable of transmitting user information to Facebook (now Meta), including for people who neither had Facebook accounts nor the app installed. He also claimed the entity had used a separate tool, CleverTap, to collect phone numbers, device models, location, time zones, usernames and internet service providers. At the time, the platform served over one million users.¹¹

NITA-U’s investigation found that SafeBoda had failed to disclose data recipients to users, that its 2017 and 2019 privacy policies omitted this information, and that it had shared data with CleverTap without specific, informed consent, in breach of the Data Protection and Privacy Act. Although its contract with CleverTap contained confidentiality provisions, no measures were in place to enforce them. Despite these findings, NITA-U imposed no sanctions, instead directing SafeBoda to address the identified deficiencies within four months and submit an action plan within two weeks, an approach reflecting a broader regulatory preference for corrective engagement over punitive enforcement.

The SafeBoda case demonstrates both the growing commercial value of personal data and the continuing weakness of data protection enforcement in Uganda. Regulators identified multiple breaches, yet the absence of sanctions points to a broader concern running through this brief: legal protections alone are insufficient unless regulatory institutions have both the capacity and the will to enforce them.

¹¹ Privacy International, “A Win for Unwanted Witness: Uganda’s Data Protection Authority Finds Ride Sharing App Unlawfully Disclosed Personal Data to Third Parties,” 11 March 2021, <https://privacyinternational.org/news-analysis/4459/win-unwanted-witness-ugandas-data-protection-authority-finds-ride-sharing-app>.

3.3 Retention, Deletion and Enforcement

Far less attention has been paid to retention, deletion and disposal than to collection. Few businesses have clear retention schedules or effective deletion protocols, so data may be retained long after it is needed, and the right to erasure remains difficult to exercise in practice. In the Albertine oil and gas region, for instance, communities have questioned what happens to data collected by companies such as TOTAL once operations wind down, highlighting the absence of clear guidance across the lifecycle of large commercial projects.

These gaps are compounded by weak enforcement of the Data Protection and Privacy Act. Regulators face significant capacity constraints in auditing, investigating and sanctioning violations, and many businesses have yet to appoint dedicated Data Protection Officers or build internal compliance systems. These shortcomings reinforce a central finding of this brief that while Uganda's legal framework establishes important safeguards, weak implementation and enforcement continue to undermine their effectiveness.

4. The Future of Work in an AI-Driven Economy

Digital labour platforms and AI-enabled technologies are creating new employment opportunities and more flexible forms of work, while exposing real regulatory gaps in labour rights, social protection, algorithmic accountability and digital inclusion. Around 18 digital labour and hybrid platforms operate in Uganda, spanning ride-hailing, delivery, freelancing, medical consultation and e-commerce, including SafeBoda, Uber, Bolt, Jumia, Glovo, Fiverr and Upwork.¹² Many rely on algorithmic management to allocate work, set pricing and, at times, deactivate workers' accounts with limited transparency or avenues for appeal.

Gender disparities remain significant. The ILO's 2024 survey of Ugandan platform workers found women averaging 50 hours of remote work weekly compared to 45 for men, yet earning USD 3 per hour against men's USD 4.40, driven by occupational segregation, unequal care responsibilities and lower access to smartphones and digital skills.¹³ Access barriers compound this: 1GB of mobile data costs USD 1.56 in Uganda, well above neighbouring Kenya's USD 0.84 and Tanzania's USD 0.68. The prohibitive data costs are further compounded by poverty - affecting 16.1% of the population and the cost of devices, which disproportionately exclude rural communities, women and informal workers.¹⁴

Meanwhile, labour regulation has not kept pace. The Employment Act, 2006, primarily protects formal employees, leaving platform workers without adequate safeguards against arbitrary, often algorithmically-triggered account deactivation, or access to social protection and occupational safety, despite Article 40 of the Constitution's broader labour rights guarantees.¹⁵

Even so, digital transformation continues to create real opportunities. Uganda's Digital Vision 2040 targets 90% digital literacy and industry-relevant skills for 70% of the population,¹⁶ and young people are already using digital tools, including AI-enabled ones, to build businesses and jobs across agriculture, finance, tourism, health and education, supported by growing innovation hubs and start-up financing. Realising this potential will require labour and digital governance to evolve alongside the technology, expanding skills while ensuring labour regulation, social protection and algorithmic accountability keep pace with how work is actually changing.

¹² ILO and Makerere University, 'Platform work in Uganda: Promoting decent work for all', 2024. Accessible at <https://www.ilo.org/sites/default/files/2024-11/24014-ILO-Digital-Labour-Uganda-report-v4-2-E.pdf>

¹³ CIPESA, *The Future of Work in Uganda* (2025), p. 3, citing International Labour Organization, *Digital Labour Platforms in Uganda* (2024).

¹⁴ *Ibid.*, p. 5, citing reporting on comparative mobile data pricing and the 2025 Uganda household survey.

¹⁵ *Ibid.*, p. 5, citing *Employment Act, 2006 and Constitution of the Republic of Uganda, 1995, Article 40.*

¹⁶ *Ibid.*, p. 6.

5. Internet Shutdowns and the Digital Economy

Internet shutdowns have emerged as one of the most significant threats to Uganda's digital economy, imposing economic, social and governance costs that extend well beyond the immediate disruption. On January 13, 2026, two days before Uganda's general election, the Uganda Communications Commission (UCC) ordered a nationwide shutdown, citing the need to curb misinformation, electoral fraud and incitement to violence. This was the third such shutdown around a Ugandan election.¹⁷

The shutdown hit an economy that, by December 2025, had 47.1 million active mobile subscriptions, 18.5 million internet subscriptions, roughly 20 million smartphones, and 36.3 million active mobile money accounts processing an estimated 27 million transactions daily.¹⁸

Healthcare, core banking, immigration and aviation systems were formally exempted, but health, fintech and e-commerce were still hit hard. Telemedicine providers such as Rocket Health lost the ability to deliver consultations, and an estimated 40% of daily digital financial transactions were disrupted. Small traders, boda boda operators and agent banking outlets, handling an estimated UGX 80.5 billion daily, were especially affected, along with youth and women who depend on digital platforms for their livelihoods.

Government services were also disrupted, including Uganda Registration Services Bureau (URSB), Uganda Revenue Authority (URA) and judiciary online systems, while exporters and traders reliant on digital systems faced delays. The Cost of Internet Shutdown Tool estimated direct losses of UGX 59.7 billion over the roughly five-day shutdown, before accounting for continued disruption to social media and mobile money, and broader damage to supply chains and investor confidence.

These shutdowns are at odds with the 2016 UN Human Rights Council resolution affirming that the same rights people enjoy offline must also be protected online.¹⁹ They also expose a gap in Uganda's 2021 National Action Plan on Business and Human Rights, which does not explicitly address digital rights.²⁰ Legal challenges to the 2016 and 2021 shutdowns remain unresolved, and the 2026 shutdown, challenged at the High Court in Kampala, still awaits a hearing.²¹ Greater collaboration between civil society and the private sector on strategic litigation could strengthen accountability through courts of law.

Ultimately, shutdowns undermine the very objectives Uganda's digital transformation agenda seeks to achieve. Beyond disrupting commerce and public services, they erode investor confidence, weaken trust in digital services and limit fundamental rights. As Uganda's economy becomes increasingly digital, reliable, uninterrupted internet access is not only a rights concern but a prerequisite for sustainable economic development.

¹⁷ "Uganda: Govt Orders Temporary Public Internet Shutdown," AllAfrica, 13 January 2026, <https://allafrica.com/stories/202601140007.html>.

¹⁸ CIPESA, "Assessing the Impact of the 2026 Internet Shutdown on Uganda's Digital Economy," April 2026, <https://cipesa.org/2026/04/assessing-the-impact-of-the-2026-internet-shutdown-on-ugandas-digital-economy/>.

¹⁹ UN Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/RES/32/13 (18 July 2016), <https://docs.un.org/A/HRC/RES/32/13>.

²⁰ Republic of Uganda, Ministry of Gender, Labour and Social Development, *The National Action Plan on Business and Human Rights* (August 2021), <https://mglsd.go.ug/wp-content/uploads/2023/07/Approved-National-Action-Plan-on-Business-and-Human-Rights.pdf>.

²¹ "MTN, Airtel, UCC Sued Over Internet Shutdown During Elections," Daily Monitor, 19 January 2026, <https://www.monitor.co.ug/uganda/news/national/mtn-airtel-ucc-sued-over-internet-shutdown-during-elections-5331438>.

Recommendations

Uganda has established important legal and policy foundations for a rights-respecting digital economy. But as this brief has shown, the rapid expansion of digital businesses, AI-enabled services and platform work has outpaced implementation, enforcement and institutional capacity. Closing that gap will require coordinated action from government, businesses, industry associations and civil society, set out below by stakeholder.

Businesses

- Strengthen data governance and informed consent: implement collection and processing frameworks build on explicit, freely given consent, backed by clear, accessible privacy notices.
- Improve data security and lifecycle management: adopt encryption, regular security audits, and clear retention, deletion and minimisation policies.
- Build organisational compliance capacity: appoint and train Data Protection Officers, embed privacy-by-design into product development, and run regular staff training on data protection, cybersecurity and phishing risks.
- Strengthen digital resilience: develop business continuity plans for internet disruptions, and collaborate with civil society and legal actors to promote an open, secure and reliable internet.

Government of Uganda

- Strengthen enforcement of the data protection framework by resourcing the PDPO and other regulators to conduct audits, investigations, and impose proportionate sanctions.
- Modernise the legal and policy framework to address biometric data, AI and platform work, aligned with constitutional and international human rights standards, and issue practical, sector-specific guidance to help businesses, particularly SMEs, comply.
- Promote digital inclusion and public awareness through sustained education campaigns, including in local languages, and continued investment in affordable infrastructure and digital skills.
- Safeguard the digital economy against internet disruptions by developing clear legal safeguards against shutdowns and ensuring any restrictions comply with constitutional and international human rights obligations.

Private Sector Associations

- Build members' capacity through regular training on data protection, cybersecurity, AI governance and business continuity planning.
- Promote industry standards and peer learning by developing model policies and compliance toolkits for consistent implementation across member organisations.
- Support risk management by encouraging periodic risk assessments among members and facilitating the sharing of lessons learned and mitigation strategies.

Civil Society Organisations

- Strengthen multi-stakeholder collaboration among government, businesses, academia and technical experts on data protection, AI governance and digital rights.
- Promote public awareness and digital rights literacy through accessible educational materials and community outreach.
- Undertake research and evidence-based advocacy on biometric data governance, AI, platform work and internet shutdowns, including documenting their social, economic and human rights impacts, to support stronger legal frameworks and strategic litigation.
- Support business compliance and resilience by developing practical guidance, templates and capacity-building support on responsible data governance.



CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Plot 10B Katalima Crescent, Naguru. | P.O.Box 122311, Kampala (U)

+256 414 289 502 | programmes@cipesa.org | [f](#) [x](#) [in](#) @cipesaug

www.cipesa.org