digital agenda

April 2026 Issue | Monthly Newsletter

The DIGITAL AGENDA Insights

DATA BECOMING A BATTLEFIELD
Page 3

Is Sovereignty Still Real in a Deeply Interconnected Digital System?
Page 8

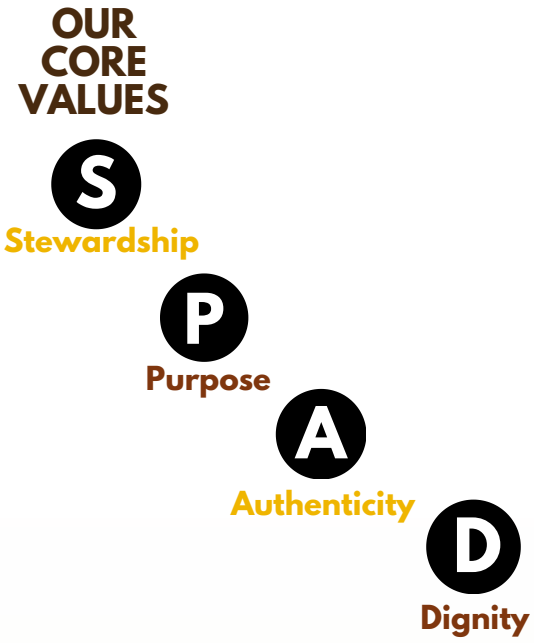
The Quiet Rebranding of Digital ID
Page 10

UGANDA'S PROTECTION OF SOVEREIGNTY BILL, 2026 - A Data and Digital Agenda Perspective
Page 5

Is Age Verification in Computer Operating Systems and Social Media Really About Children's Safety?
Page 9

The Centralisation Paradox: Why Data Breaches Aren't Slowing Centralisation Policies
Page 11

Tech Should Serve Not Control



Welcome to THE DIGITAL AGENDA INSIGHTS monthly newsletter

This edition reflects a growing shift in how we understand technology. Data is no longer just about innovation or convenience. It is becoming a space of power, control, and contest.

From Uganda's Protection of Sovereignty Bill to age verification systems and the quiet expansion of digital identity, a pattern is emerging. Systems presented as tools for safety, efficiency, and inclusion are also increasing visibility, centralisation, and dependence.

At the same time, repeated data breaches continue to expose the risks of concentrating sensitive information, yet policy continues to press forward in the same direction, with no sign of retreat.

This raises a deeper question: in a deeply interconnected digital system, what does sovereignty really mean, and who truly holds control?

This edition does not offer definitive answers. It invites you to question the assumptions behind the digital agenda and to consider the long-term implications of the systems being built today.

If our work resonates with you, please join us. Also, partner with us.

Lilian Agaba Nabwebale

For Digital Agenda Forum

DATA BECOMING A BATTLEFIELD

On 01 April 2026 at 7:00 PM, the Digital Agenda Forum hosted an X Space discussion on the theme **DATA BECOMING A BATTLEFIELD**

Moderators: Maria Batenga, a Tech Practitioner | Digital Rights Activist, and Claire Babirye, a Data Scientist.

Panelists: Abaasa Peace Ella - Security Operations Center Analyst; Arthur Olowo - Digital Policy Analyst and Strategist; David Iribagiza - Digital Rights Advocate and Lawyer and Saint Mogogi Timothy Moliwa - Prophet of God from Botswana.

Executive Summary

The discussion recognised that warfare is no longer confined to physical battlefields involving tanks and troops. Instead, a fundamental shift has occurred: data, digital infrastructure, and information systems have become the new frontiers of conflict. Nations and non-state actors now wage wars using cyber attacks, surveillance, and disinformation, targeting civilians and their personal data as primary weapons. Power has moved from oil-rich nations to tech giants and state actors who control data ecosystems.

Key themes included the inadequacy of current legal frameworks, the dangers of over-centralised Digital ID systems, and the necessity of integrating a human rights-based approach with proactive faith-based leadership to safeguard human dignity.

1. The Shift in Power: From Oil to Data

Control of data ecosystems now influences economies, geopolitics and public opinion more than oil once did. Nations and non-state actors now use cyber operations, surveillance, and disinformation as primary weapons of influence and conflict.

2. Legal & Human Rights Gaps (David Iribagiza)

While laws such as Uganda's Data Protection and Privacy Act exist, they are often ignored by state actors. For example, during the recent national ID renewal exercise, citizens were forced to provide iris scans and extensive biometric data without giving free or informed consent. Access to essential services like healthcare and tax filing was made conditional on submitting this data, which violates the legal principle of data minimisation, that only necessary information should be collected, and only with genuine consent.

Solution: Enforce transparency, accountability, and data minimisation. Citizens can use strategic litigation and file complaints with bodies like the Personal Data Protection Office (PDPO) to hold both government and private entities accountable.

3. Cyber Attack Evolution (Abaasa Peace Ella)

Cyber attacks have evolved from financially motivated crimes to coordinated geopolitical strategies. A striking example occurred during the Iran-Israel conflict, where Israeli civilians received text messages offering links to real-time information about bomb shelters. In moments of panic and fear, people clicked these links, only to download spyware that gave attackers access to their cameras, locations, and sensitive personal data.

Attackers exploit human psychology; panic, fear, and urgency, not just technical system flaws.

Resilience Strategy: Build "muscle memory" through continuous, weekly cyber

awareness training rather than one-off annual workshops.

Also, avoid over-centralisation, where identity systems, banking, telecoms, and health records are all linked together, because this creates a single point of failure. If one system is breached, attackers can move across the entire ecosystem. Systems should have segmentation, manual fallbacks, and controlled independence.

4. Digital Identity & Central Bank Digital Currencies (Arthur Olowo)

Integrated systems that link Digital IDs with Central Bank Digital Currencies (CBDCs) could lead to mass surveillance and financial exclusion. For example, if your digital ID is linked to your money, the government could potentially monitor every transaction you make; what you buy, where you go, and who you pay. More concerning, if you fall out of favour with authorities, you could be locked out of the financial system entirely, unable to buy or sell anything.

Laws must prioritise user consent and protection over government convenience. Systems need "privacy by design" (such as zero-knowledge proofs that verify identity without exposing personal data). Above all, decisions about technology must remain human-centric, not purely efficiency-driven.

5. Faith-Based Perspective (Saint Mogogi)

Proposition: "My people perish for lack of knowledge." Fear and ignorance have silenced spiritual voices, causing many to view all technology as demonic rather than engaging with it as stewards.

Role of Prophecy: Prophecy provides firsthand intelligence, prior knowledge of coming events, to help anticipate rather than merely react to developments like the rise of CBDCs or digital surveillance systems.

Action: The faith community must break the cycle of fear, proactively influence policy, and utilise the "spirit of a sound mind" rather than fear of technology. Believers are called to be the light of the world, meaning they should know things firsthand and speak into the systems shaping society.

AUDIENCE Q&A HIGHLIGHTS

On Government Over-Collection: Citizens can enforce data minimisation laws via strategic litigation and reporting to the PDPO. Courts can compel the government to stop unlawful collection practices.

On the Agenda Behind Data Conflict: The agenda is moving from physical economy leverage to predictive control, using collected data to map, predict, and manipulate human behaviour for political and economic gain.

CALL TO ACTION:

1.Citizens: Should demand accountability from data collectors, practice continuous cyber hygiene, and report violations to the PDPO.

2.Policymakers & Government Agencies: Must enact laws that enforce data minimisation and transparency, while also refraining from over-integrating critical systems (e.g., linking IDs to banking, healthcare, business registration, document authentication, tax identification (URA TIN), and property ownership records),. Must also ensure that consent is genuinely free and informed rather than a precondition for essential services.

3.Faith & Civil Society: Must break the cycle of fear by using prophetic insight, legal expertise, and policy advocacy to anticipate and shape digital policy, ensuring that technology honours human dignity and divine order.

CONCLUSION

Data has become a battlefield where civilians are the primary targets. Resilience is not built during a crisis but long before it happens, through awareness, legal safeguards, and spiritual readiness.

Find the Recording at:
https://youtu.be/x5nnsmb0vMo?si=ILHZZK1tqZ-0XPgE

By DIGITAL AGENDA FORUM
www.thedigitalagenda.org

@DigitalAgendaT

UGANDA'S PROTECTION OF SOVEREIGNTY BILL, 2026

- A Data and Digital Agenda Perspective

On 22 April 2026 at 7:00 PM, the Digital Agenda Forum hosted an X Space discussion titled **UGANDA'S PROTECTION OF SOVEREIGNTY BILL, 2026 - A Data and Digital Agenda Perspective.**

Moderators: Lilian Agaba Nabwebale, Information Scientist and Claire Babirye, Data Scientist

Panelists:

- Honorable Christopher Komakech – Member of Parliament for Aruu County
- Honorable Alex Brandon Kintu – Member of Parliament for Kagoma North County
- Morgan Muhindo – Lawyer, Data Protection & Privacy Expert, Fintech Specialist, Co-founder of Enset Law
- Eden Kironde – Host, Weapons of War podcast (socio-political analysis)

1. OVERVIEW

The discussion examined Uganda's Protection of Sovereignty Bill, 2026 from a digital, data, and technological perspective. The panel explored whether the bill addresses modern sovereignty challenges, namely data infrastructure, cross-border data flows, digital rights, and technological dependence, or whether it serves primarily to expand state control.

2. KEY CONCERNS RAISED

2.1 Digital Sovereignty Gap

- The bill focuses narrowly on financial and economic aspects but is silent on data protection, data localisation, and cross-border data flows.

- Uganda's government systems and digital economy rely heavily on foreign cloud services, platforms and undersea cables. The question is: can sovereignty be legislated without addressing digital infrastructure?

2.2 Broad and Vague Definitions

- "Foreigner" includes Ugandan citizens living abroad, dual citizens, and foreign entities.
- "Agent of a foreigner" is defined so broadly that relatives receiving remittances, employees of international organisations, NGOs, religious groups, and even online content creators could fall under its scope.
- No minimum financial threshold is specified, meaning even small payments (for example, $50) could trigger registration requirements.

2.3 Chilling Effects on Rights

- ***Freedom of expression and online discourse:*** the bill could criminalise opinions seen as undermining government policy or economic stability.
- ***Freedom of worship:*** religious institutions receiving funds from diaspora members may need licences, potentially limiting offerings and donations.
- ***Digital rights:*** the bill overlaps with the now partially struck down Computer Misuse Act, raising fears of renewed suppression of online assembly and speech.

2.4 Economic and Fintech Impact

- Capping funds received from foreign sources at UGX 400

million per annum (approximately $107,000) without proper licensing could cripple:
    - Startups and fintechs relying on foreign investment;
    - Banks accessing international credit lines;
    - Remittances from the diaspora (a major source of household income).
- Panelists argued this undermines economic sovereignty rather than protecting it, especially given Uganda's high dependence on foreign aid and imports.

2.5 Inconsistencies with Existing Laws and Agreements

- The bill duplicates provisions already in the Anti-Money Laundering Act and Anti-Homosexuality Act.
- A recent US-Uganda health data sharing agreement (which gives the US real-time access to sensitive health data) was cited as a direct contradiction: the government cannot claim digital sovereignty while signing away data rights.

2.6 Legislative Process and Constitutional Risks

- Hon. Komakech noted the bill is at committee stage, with public submissions open until 24 April 2026.
- Other panelists warned that vague laws lead to constitutional challenges (like the Computer Misuse Act) that take years to resolve, during which citizens may be prosecuted.
- Morgan Muhindo stated: "This bill is irredeemable…its purpose and effect are unconstitutional."

> **This Bill is irredeemable.**
> ***~ Morgan Muhindo***

3. DIVERGING PERSPECTIVES

Hon. Komakech (Government-aligned)

- Bill aims to protect Uganda from foreign manipulation and rogue funding (for example, LGBTQ+ agendas, economic sabotage).
- Technology issues can be addressed later via ministerial regulations.
- Citizens can challenge the law in constitutional court if passed.
- The cap at UGX 400M only affects large, suspicious transactions.

Morgan, Eden, and Participants (Critical)

- Bill is a tool for self-preservation of the ruling party, not national sovereignty.
- Excluding digital governance from the core bill renders it incomplete and dangerous.
- Court challenges take three to five years; livelihoods and freedoms are destroyed in the meantime.
- No minimum threshold means even small remittances could require registration.

4. AUDIENCE QUESTIONS AND RESPONSES

- On faith matters such as Prophet Elvis Mbonye's prophecies on GAVI funding and donor withdrawals, the audience questioned whether they could be construed as economic sabotage or lead to indirect censorship. Hon. Komakech responded that prophecies have no legal bearing and the bill does not target worship, while critics argued this was not clearly reflected in the Bill.
- On citizens receiving funds from diaspora: the bill has no minimum threshold, so for any amount, theoretically registration could be required.
- Why a new law instead of amending existing ones? Hon. Komakech argued the bill is needed now to address financial gaps. Critics said existing laws already cover the stated concerns.

5. TAKEAWAYS AND NEXT STEPS

- Hon. Komakech: will take back to Parliament the need to explicitly include technology and data clauses. Encouraged citizens to make written submissions to the Clerk of Parliament by 24 April 2026.
- Eden Kironde: the bill is rooted in fear and control, not liberty. Urged citizens to remain hopeful but prepared for a better future.
- Morgan Muhindo: called on legislators to reject the bill entirely, warning it sets a dangerous precedent for democracy, economics, and Pan-African solidarity.

6. CONCLUSION

The debate exposed a stark divide, with government presenting the bill as protective sovereignty while experts warn it is a vague, overbroad instrument that risks harming key sectors and freedoms, urging public engagement before the 24 April 2026 deadline.

Recording at
https://youtu.be/M4LRg8DG15Q?si=uzJJ3cwDNmOIyZhr

By DIGITAL AGENDA FORUM
www.thedigitalagenda.org

@DigitalAgendaT

Digital Agenda Forum Submits Memorandum on the Protection of Sovereignty Bill, 2026 from a Digital and Data Governance Perspective

Following the Clerk to Parliament's public notice inviting submissions on the Protection of Sovereignty Bill, 2026 by Friday, 24 April 2026, the Digital Agenda Forum duly submitted its memorandum on the same day. The submission, addressed to the Joint Committees on Defence and Internal Affairs and on Legal and Parliamentary Affairs, presents a focused analysis of the Bill from a digital and data governance perspective.

Our guiding position is that sovereignty is not exercised in isolation, but within a deeply interconnected global digital environment. Effective sovereignty, therefore, requires clarity, precision, and alignment with digital realities.

From this standpoint, our submission highlighted specific areas where the Bill may fall short, including overly broad and ambiguous definitions, limited recognition of how modern digital systems and cross-border data flows operate, and a regulatory design that risks overreach through centralised control and wide discretion.

We proposed a more targeted, risk-based and technically grounded approach that focuses on demonstrable harm, safeguards legitimate digital and civic activity, and ensures the law remains enforceable in practice.

Digital Agenda Forum
Plot 47, Kigo Lweza, Kampala, Uganda
+256 782 408607
info@thedigitalagenda.org
P.O BOX 172431, Kampala, Uganda
www.thedigitalagenda.org

0755419853
0414377155

RECEIVED
24 APR 2026
IN PRMS

Our Ref: P2026-04-0001

Date: 24th April 2026

TO: THE CLERK TO PARLIAMENT
Parliament of the Republic of Uganda
Room S108, South Wing, Parliamentary Buildings
Kampala-Uganda

Dear Sir,

RE: SUBMISSION OF A MEMORANDUM ON THE PROTECTION OF SOVEREIGNTY BILL, 2026

Digital Agenda Forum respectfully submits the attached Memorandum for the consideration of Parliament, providing a structured digital governance and data policy perspective on the Protection of Sovereignty Bill, 2026.

The submission highlights key areas where legislative refinement is recommended to ensure that the Bill is precise, enforceable, and aligned with the realities of Uganda's digital and interconnected environment.

We trust that the insights provided will contribute constructively to the legislative process.

SUBMISSION TO THE JOINT COMMITTEE ON DEFENCE AND INTERNAL AFFAIRS AND LEGAL AND PARLIAMENTARY AFFAIRS TO PARLIAMENT

MEMORANDUM ON THE PROTECTION OF SOVEREIGNTY BILL, 2026

A DIGITAL AND DATA GOVERNANCE PERSPECTIVE

PRESENTED BY **DIGITAL AGENDA FORUM**

1. ABOUT DIGITAL AGENDA FORUM

The Digital Agenda Forum is a Technology civic platform based in Kampala, Uganda, dedicated to shaping discourse and policy at the intersection of technology, society, and governance.

The Forum convenes professionals, thought leaders, and practitioners across technology, law, policy, and civil society to engage on emerging digital issues, influence public policy, and contribute to national and global conversations on the digital future.

Its work is anchored in the principle that technology must serve people, not control them, promoting approaches to digital transformation that respect human values, uphold ethical standards, and protect fundamental rights.

Through policy briefs, open letters, public discussions, and research-driven engagements, the Forum contributes practical, context-aware perspectives to legislative and regulatory processes, particularly in areas such as digital identity, data governance, privacy, and emerging technologies.

2. INTRODUCTION

This Memorandum is respectfully submitted to Parliament to provide a high-level digital governance and data policy perspective on the Protection of Sovereignty Bill, 2026.

The Bill is driven by a legitimate objective: safeguarding Uganda from harmful foreign interference and preserving national sovereignty. This objective is both valid and necessary.

However, sovereignty today operates within a deeply interconnected global digital environment. Uganda's economy, governance systems, and civic life are increasingly dependent on cross-border data flows, digital platforms, and financial systems.

Accordingly, sovereignty is exercised not in isolation, but within these global systems.

3. GUIDING POSITION

It is our considered position that effective sovereignty requires clarity, precision, and alignment with digital realities.

Regulation of foreign influence must therefore be targeted and enforceable, while avoiding unintended disruption to legitimate digital, economic, and civic activity.

Detailed Memorandum at
https://thedigitalagenda.org/wp-content/uploads/2026/05/Digital-Agenda-Forum-Memorandum-on-Protection-of-Sovereignty-Bill-2026.pdf

Is Sovereignty Still Real in a Deeply Interconnected Digital System?

By **Lilian Agaba Nabwebale,**
Information Scientist

As societies become more digital, essential services like banking, healthcare, transport, communication, and access to government support are more and more tied to central systems. Identity checks, mobile money, digital records, and online platforms are becoming the main ways people take part in everyday life. On the surface, this is about faster services, less fraud, and easier access for more people.

A deeper question comes up when these systems are no longer optional. What happens when they become the only way to access basic needs? If people must go through central digital systems to live, work, and survive, what protections are in place to make sure no present or future authority can use that power to control beliefs, silence people, or exclude others because of their conscience, religion, or faith?

This question becomes more important when laws about sovereignty and national control are introduced in a world that is already highly digital and connected. Such laws are often presented as ways to protect the country, manage outside influence, and strengthen national control. These are normal concerns for any state. However, people begin to worry when such laws are broad, especially at a time when civil society, media, business, and daily life all depend heavily on digital systems.

The concern is not just about what these laws say, but how they work in real life. If access to money, organisations, digital platforms, or even international connections depends on identity systems and compliance rules, then questions arise. Who controls access? Who decides? Can someone be excluded, whether on purpose or by mistake?
This is not about rejecting technology or saying there should be no laws. Digital systems and regulation are needed. At the same time, it is important to understand that when people depend heavily on a system, the power of that system grows.

History shows that systems usually start with good intentions like improving efficiency and order, and over time, if not carefully managed, they can become a forceful central ideology that everyone must follow and cannot exist without it.

a forceful central ideology that everyone must follow and cannot exist without it.

For people of faith and conscience, this is especially important. Faith often requires people to live according to their beliefs, even when those beliefs are not popular or do not fit into systems. People should be able to live, work, and take part in society without being forced to go against what they believe.

So the real question is not whether digital systems or sovereignty laws should exist, but how they are designed and controlled. Are there alternatives to access essential services if someone cannot use the main system? Are there strong protections to stop people from being unfairly excluded? Are the systems transparent and accountable? And most importantly, is there still space for people to live according to their conscience?

A strong society is not only one that uses technology and makes laws. It is one that makes sure no single system has full control over people's ability to live, participate, and remain free in what they believe.

Is Age Verification in Computer Operating Systems and Social Media Really About Children's Safety?

By **Mariagorreti Batenga,**
Tech Practitioner | Digital Rights Activist

Recently, there has been a lot of discussion about children and social media, and many people are quickly jumping to government bans, digital restrictions, and even digital IDs as solutions, at a time when concerns about digital control are already growing.

While protecting children is a genuine concern, and social media has exposed them to confusion, identity crises, hyper-sexualisation, peer pressure, addiction, and distorted realities during a critical stage of development, it does not mean the solution should be surrendering to digital control. Once children's safety becomes the justification for online restrictions, it becomes easy for those seeking control to introduce systems that go beyond protection.

It starts as "protect the children," and then the next day it becomes mandatory to provide identification to access these platforms. It builds up into digital surveillance and an infrastructure of control that affects everyone.

In the UK, where conversations about protecting children online are gaining momentum, many people are beginning to notice that under the guise of child safety, there is a growing push towards age verification systems and identity-linked internet access. Australia has already passed a law requiring online age checks. California has also passed a law applying age verification at the device and operating system level. Europe is pushing for the same.

In Uganda, a viral video of schoolgirls in uniform sharing explicit messages from their "boyfriends" sparked outrage, mainly directed at schools and social media, with little focus on parents. Some also suggested requiring ID to access social media. While platforms may amplify such behaviour, they do not raise children from infancy. Schools and society have a role, but the home remains the foundation, not the government.

There is need for caution, not because children's safety is unimportant, but because genuine concerns can be used to normalise systems that drift from their original purpose. Our response should not be to shift responsibility to control systems, but to address the real issue in many cases: parenting itself.

It is easier to call for banning children under 15 from social media than to ask how they got there in the first place. Why do they have unrestricted smartphones, open internet access, and unlimited app downloads without proper parental controls? In many cases, parents are not setting boundaries, sometimes even treating unrestricted access as a status symbol or social approval, and then shifting responsibility to broad restrictions that risk digital control for everyone.

Do children walk into shops alone, sign contracts, and buy expensive phones themselves? If not, then phone sellers could also be held accountable. A child should need an adult to purchase a phone for them, and that adult should ensure proper restrictions are set before handing it over.

We cannot ignore this: adults are the gatekeepers. They provide the devices but are often too distracted or negligent to supervise what their children consume, and sometimes even use these platforms to keep children occupied. Yet they blame platforms, schools, and governments, while avoiding their own responsibility.

Technology can never replace parenting. A device is a tool that can educate or harm depending on who controls it. Social media can educate, connect, and create opportunities, but without guidance it can also harm children. If a parent feels a child is not ready, they should use parental authority to delay phones, restrict apps, and monitor use, rather than pushing for broad government controls that affect everyone.

The Quiet Rebranding of Digital ID

Digital identity is no longer a project; it is an ecosystem that hides in plain sight through its applications. It is not presented as a centralised system of control, but as multiple solutions to unrelated problems.

Digital identity is no longer introduced as digital identity. The term itself has become almost invisible in public messaging, replaced by a rotating set of softer, more acceptable narratives that conceal its expanding scope. What once would have been a straightforward discussion about population-wide identification systems is now dispersed across child safety, financial inclusion, cybersecurity, service delivery, and even environmental policy.

Instead of saying "register everyone," the language now speaks of protecting children online through age verification systems embedded in social media platforms and operating systems. Instead of "central identity databases," the focus shifts to seamless access to government services, fraud prevention, and eliminating paperwork. Border control is reframed as digital security and the need to verify foreigners in an increasingly interconnected world. Even broader national systems such as Electronic Vehicles rollout programmes, digital number plates, mobile money regulation, and telecom registration are gradually tied into the same underlying logic of verified identity and traceable participation in public systems.

Each layer appears justified on its own. Child safety feels separate from tax compliance. Fraud prevention feels separate from industrial policy. Transport innovation feels separate from national security. Yet beneath these distinct policy goals sits a growing pattern of convergence, where identity becomes the silent connector between systems that were once independent. The result is not a single programme called digital ID, but a distributed architecture of verification embedded across everyday life.

This is what makes it difficult to clearly define. Digital identity is no longer a project; it is an ecosystem that hides in plain sight through its applications. It is not presented as a centralised system of control, but as multiple solutions to unrelated problems. The fragmentation of language makes it easier to accept each piece individually, while the combined effect becomes visible only when the systems begin to interlock.

The challenge, therefore, is not only technological but linguistic. As long as digital identity continues to be disguised as safety, efficiency, and innovation, it remains difficult to see as a single coherent structure. Yet it is precisely this fragmentation of meaning that allows it to expand quietly across sectors, borders, and everyday digital interactions without ever needing to be named directly.

By DIGITAL AGENDA FORUM

The Centralisation Paradox: Why Data Breaches Aren't Slowing Centralisation Policies

As 2026 progresses, a stark picture is emerging across the digital landscape. No sector appears untouched by rising cyber intrusions, with 486 breach events recorded in the first quarter alone. In France, the national identity system ANTS saw around 19 million records exposed, including names, addresses, birth dates and civil status, with reports of the data being sold on the dark web. The FICOBA bank registry was also breached, affecting about 1.2 million bank-linked records, directly impacting financial infrastructure.

Telecommunications systems have proven equally vulnerable: Canada's Telus faces claims of 700 terabytes of stolen data, including personal information, call data and background checks, while US provider Brightspeed reported a ransomware attack exposing data of over one million customers.

The technology and cloud sectors are also heavily affected. Vercel suffered a data leak exposing employee information, emails and logs, linked to a compromised third-party AI tool. A major cloud misconfiguration left a database of 149 million records publicly accessible. Social platforms were hit as well, with South Korea's Duo matchmaking service breached, affecting about 420,000 users and exposing sensitive data such as phone numbers, marital history, addresses and workplaces.

Healthcare remains a key target. Catalyst RCM, a US medical billing provider, was hit in a wider wave of attacks on health systems. Additionally, the UK Biobank, which holds health records for approximately half a million individuals, has had its de identified data listed online.

Looking across these incidents, several patterns emerge. No sector is safe, with government, telecom, healthcare, education and finance all affected.

High-value institutional data is also under threat. In 2026, leaks involving Harvard University and the University of Pennsylvania exposed over one million personal records, including home addresses, financial and donor information, and demographic data. The financial sector was also hit, with fintech firm Finastra losing around 400GB of sensitive data, while the ADFW leak exposed passports and ID documents via an open server linked to a global financial summit. Industrial systems were not spared, as Nissan suffered a ransomware attack affecting corporate systems and potentially sensitive data.

Looking across these incidents, several patterns emerge. No sector is safe, with government, telecom, healthcare, education and finance all affected. Identity systems are prime targets, as national IDs, telecom records and banking registries form the backbone of digital access and control, making them highly valuable. Third-party tools are a major weak point, with breaches often occurring through dependencies such as AI tools, cloud misconfigurations, and OAuth or login integrations rather than direct attacks. Finally, there is a clear shift in tactics: data is increasingly exfiltrated, sold and leaked, rather than simply encrypted for ransom, with attackers focusing on copying and monetising it.

However, even as breaches multiply and expose the risks of

storing vast volumes of personal data in centralised systems, many countries are pushing further in the same direction. The very infrastructures being compromised are the ones governments continue to expand and reinforce. Instead of shifting towards decentralised or privacy-preserving alternatives, policymakers appear to be doubling down on consolidation.

Despite the growing evidence of systemic vulnerability, policy direction remains largely unchanged. In some cases, it is even strengthened, with governments continuing to justify expanded centralised data architectures as necessary for efficiency, security, and service delivery. The result is a cycle where exposure does not slow consolidation but becomes part of the rationale for it.

The result is a paradox: incidents that highlight the fragility of centralised databases are also used to justify their expansion. The lesson of 2026 so far is increasingly clear. Centralised personal data systems have become a battlefield, yet the response is to build larger repositories, concentrate more sensitive information into single digital vaults, and hope for the best. It is a striking contradiction, one that hackers and data brokers are likely observing with interest.

The bottom line is that 2026 is making it clear that personal data systems themselves are becoming the battlefield. These are not merely financial hacks, but acts of identity leverage, intelligence gathering, and attempts to gain control over key systemic points.

The irony is that, despite repeated breaches, many nations are moving further towards the same centralised data architectures that have proven so vulnerable. The paradox remains unresolved: the evidence warns against concentration, yet policy continues towards it.

Whether this is resilience or risk will depend on whose data is exposed next.

By
DIGITAL AGENDA FORUM

The irony is that, despite repeated breaches, many nations are moving further towards the same centralised data architectures that have proven so vulnerable.

The paradox remains unresolved: the evidence warns against concentration, yet policy continues towards it.

Whether this is resilience or risk will depend on whose data is exposed next.

Faith and the Digital Agenda

Prophecy Exposes Alarming Globalists Digital Currency Plot

On 7th January 2025, Prophet Elvis Mbonye spoke of a coming strategy by global powers — a digital financial system masked as innovation and security but designed for control. The prophecy revealed the UK as the launch point for central bank digital currencies (CBDCs), soon extending to Africa through Kenya, Ghana, and Nigeria. One week later, the world watched as these events began to manifest — digital pound initiatives, global ID systems, and regulatory frameworks echoing the prophetic word. As foretold, what was meant for bondage is now being unveiled, proving once again the divine grace and authority upon the prophet of this generation.

Watch

Find all the previous Newsletter editions at www.thedigitalagenda.org/newsletter

Reach us on e-mail at ***info@thedigitalagenda.org***

Join Us in Shaping the Future of Digital Technology!

WAYS YOU CAN PARTICIPATE

1. **Support Us Financially** — Partner with us through donations or sponsorships to advance the Digital Agenda Forum's vision.
2. **Be a Panelist** — Share your expertise and insights during our Townhalls.
3. **Join the Live Audience** — Participate in our Townhalls, engage with speakers, and contribute your views in real time.
4. **Write for Our Newsletter** — Submit thought-provoking articles for The Digital Agenda Insights Monthly Newsletter.
5. **Shop with Us** — Purchase items from our online shop to support our initiatives while showcasing the Digital Agenda Forum
6. **Follow and Share** — Stay connected through our social media platforms and website. Engage with our posts and share our content widely to spread the message.

Partner with us today and be part of a movement that's shaping a digital future for all!

Reach us on e-mail at ***info@thedigitalagenda.org***

This is a Publication of Digital Agenda Forum

Contact Us

For further inquiries and information

Digital Agenda Forum
📍 Munyonyo, Kampala, UG
📞+256 782 408607
✉️ *info@thedigitalagenda.org*
✉️ P.O BOX 172431, Kampala
🌍 www.thedigitalagenda.org

@DigitalAgendaT