Free Tech-Law Webinar

Accountability, Governance & Ethical Boundaries:

Who Bears Responsibility for AI-Generated Harm?

Adeniyi Ajose
Data Protection Manager
Experienced Data Analyst

Chidera Didigu
Founder
Clearpoint Legal

Ayomide Ahmed
Senior Associate
Equibridge Attorneys (EBA)

Thursday, 05 March 2026

03:00 pm - 04:30 pm WAT

Virtual (Google Meet)

Dipo Ige
Moderator

https://forms.gle/m8EYbFFxqB1bjdZw5

AI WEBINAR REPORT

On 5 March 2026, **LawDigits** convened a high-level webinar bringing together experts in data protection, digital governance, and technology law to discuss the emerging issue of accountability for harm caused by artificial intelligence systems.

The webinar examined how responsibility should be allocated across the AI ecosystem and considered the implications for countries such as Nigeria that largely depend on foreign-developed AI technologies.

The discussion highlighted the rapid evolution of technological systems, moving from earlier forms of digital communication to highly advanced artificial intelligence models capable of generating content, automating decisions, and influencing social, economic, and governance structures. While these technologies offer transformative benefits across sectors including healthcare, finance, law enforcement, and education, they also introduce significant legal and ethical risks.

admin@thelawdigits.com

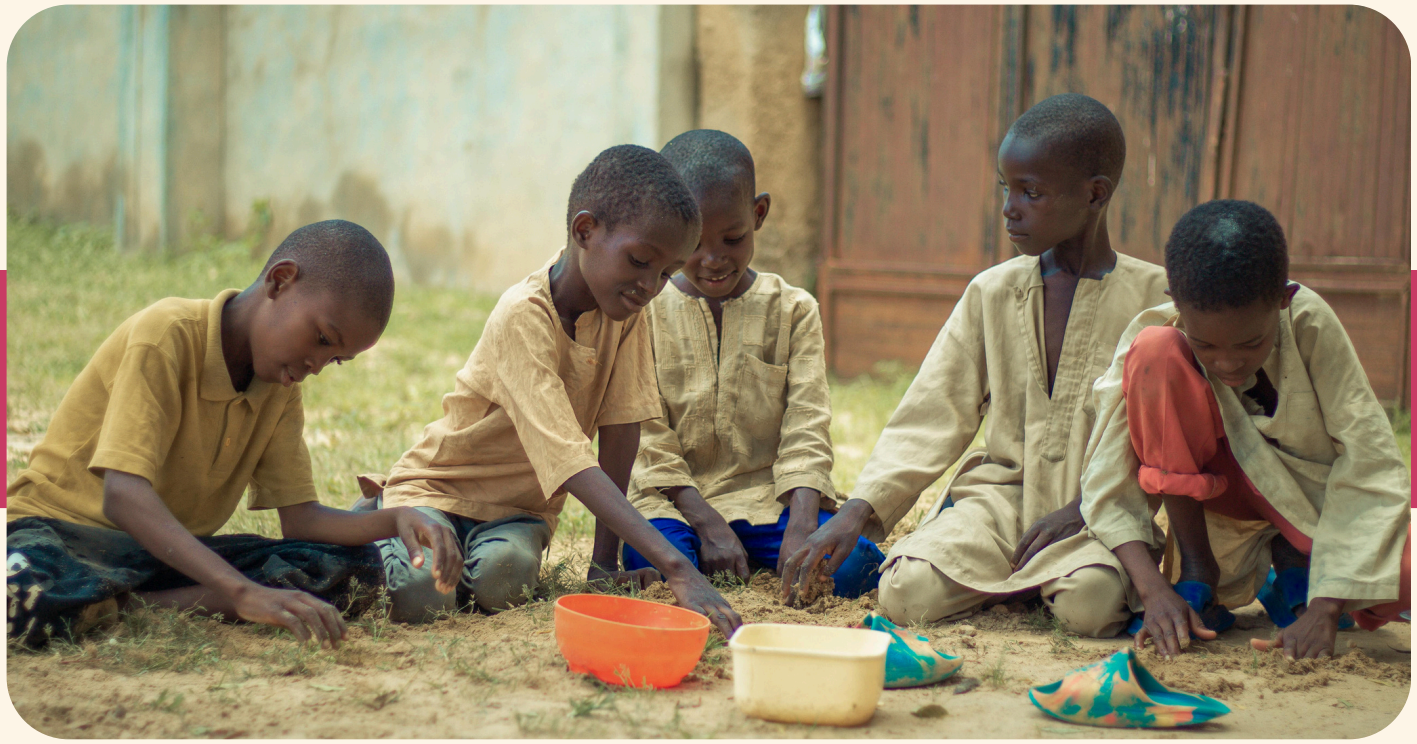
READ MORE

Speakers emphasized that the question of accountability for AI-generated harm is complex, particularly where multiple actors participate in the development, deployment, and use of AI systems. These actors include technology developers, service providers, corporate deployers, regulators, and end users. Determining liability therefore requires a careful examination of control, foreseeability of harm, and benefit derived from AI outputs.

A major theme of the discussion was Nigeria's dependence on foreign AI infrastructure, which raises significant concerns about data sovereignty, regulatory oversight, and national security. Because many AI systems are developed and hosted outside Nigeria, enforcing local regulatory standards or holding foreign technology companies accountable presents practical and legal challenges.

The panel also explored possible avenues for citizen redress, including complaints to the Nigeria Data Protection Commission (NDPC) and reliance on constitutional privacy protections. However, speakers noted that long-term solutions require **structural reforms**, including **domestic investment** in technology infrastructure, **improved regulatory frameworks**, and **increased public awareness** about digital rights.

The webinar concluded that education, infrastructure development, regulatory cooperation, and responsible AI governance are critical to ensuring that artificial intelligence can be deployed safely while minimizing harm to individuals and society.



Detailed Discussion and Analysis

The Rapid Evolution of Technology and the Rise of AI Risks

1

The webinar opened with a reflection on the rapid transformation of technology over the past several decades. Society has moved from relatively simple communication systems to a deeply interconnected digital ecosystem powered by artificial intelligence.

AI technologies now play a role in:

- Healthcare diagnostics
- Financial systems
- Legal analysis
- Law enforcement
- Education
- Online platforms and digital communication

Despite these benefits, the panel acknowledged that AI systems introduce several serious risks, including:

Algorithmic bias

AI systems trained on biased data may reinforce discrimination and produce unfair outcomes.

Hallucinations and misinformation

Generative AI systems may produce inaccurate or fabricated information presented as factual.

Privacy violations

AI training datasets may include personal data collected without adequate consent.

Intellectual property infringement

Creative works may be used to train AI models without permission from authors or rights holders.

These risks raise critical questions about who should bear legal responsibility when AI systems such as these, cause harm.

2 The Rapid Evolution of Technology and the Rise of AI Risks

One of the most significant themes of the discussion was the strategic vulnerability created by Nigeria's reliance on foreign AI technologies.

Data Sovereignty Concerns

Adeniyi Ajose emphasized that Nigeria functions primarily as an end-user of AI systems developed abroad. As a result, Nigerian data is often used to train foreign models without Nigeria exercising meaningful control over the algorithms or decision-making processes involved.

True data sovereignty, according to the panel, requires more than local data storage. It includes:

- Algorithmic transparency
- Auditability of AI systems
- Local regulatory authority
- Strategic technological autonomy

Without these elements, countries may lose control over how their citizens' data is used.

National Security Implications

Ayomide Ahmed highlighted that reliance on foreign AI systems may also pose national security risks. If critical infrastructure relies on external technologies that are not subject to domestic oversight, governments may lack the technical capability to manage risks effectively.

3 Infrastructure Challenges and Technological Limitations

Another key issue discussed was the infrastructure deficit limiting Nigeria's ability to build domestic AI systems.

Developing advanced AI systems requires:

- Large-scale computing infrastructure
- High-capacity data centers
- Reliable electricity supply
- Substantial water resources for cooling servers
- Highly specialized talent

Speakers noted that the energy consumption required to operate a single AI data center may exceed Nigeria's current national electricity capacity, highlighting the magnitude of the challenge.

These constraints have contributed to a brain drain, where talented Nigerian engineers and developers relocate abroad to build and deploy advanced technologies.

LawDigits
Education | Research | Innovation

About Us

LawDigits is a research, consultancy, and training hub designed to meet the urgent needs of Nigeria's legal and regulatory landscape, especially in the area of Data Protection, Digital Rights, Artificial Intelligence and Cybersecurity.

Follow us on:

LinkedIn

4 Accountability Across the AI Value Chain

The central legal question explored during the webinar concerned who should bear responsibility for AI-generated harm.

The AI Value Chain Model

Chidera Didigu argued that accountability should be assessed along the AI value chain, which includes:

1. Developers – entities that design and train AI systems
2. Providers – companies that supply AI tools
3. Deployers – organizations that integrate AI into their services
4. End users – individuals who interact with the technology

Under this framework, responsibility depends on:

- The degree of control exercised by each actor
- The foreseeability of potential harm
- The benefits derived from the AI system

Concurrent Responsibility

Adeniyi Ajose further argued that accountability does not need to be exclusive. Instead, multiple actors may share responsibility simultaneously.

For example:

- Developers must design safe systems.
- Deployers must use the technology responsibly.
- Users must avoid misuse of AI tools.

This layered accountability structure is consistent with existing legal principles in areas such as product liability and negligence law.

5 Regulatory Enforcement Challenges

A significant barrier to effective AI regulation is the difficulty of enforcing local laws against multinational technology companies.

Speakers noted that even powerful global regulators sometimes struggle to enforce penalties against large technology firms.

Potential consequences of aggressive regulation include:

- Withdrawal of services from certain markets
- Reduced access to technology
- Limited cooperation from multinational companies

This creates a difficult balancing act for governments seeking to protect citizens while maintaining access to global technological innovations.

6 Citizen Redress and Legal Remedies

The panel identified several existing mechanisms through which Nigerians may seek redress for AI-related harm.

Nigeria Data Protection Commission (NDPC)

Individuals may file complaints with the NDPC where AI systems misuse personal data. The Commission has investigative and enforcement powers under Nigeria's data protection framework.

Constitutional Privacy Rights

Section 37 of the Nigerian Constitution protects the right to privacy, which may be invoked when AI systems improperly collect or process personal data.

7 Protecting Intellectual Property in the Age of AI

The panel also examined how AI systems challenge traditional intellectual property frameworks.

AI models frequently rely on large datasets containing copyrighted works, raising questions about whether authors and creators should receive compensation.

Speakers referenced international approaches including:

- EU AI Act transparency requirements
- Documentation of training data sources
- Licensing models for creative works

However, enforcement remains difficult where foreign AI developers operate outside local jurisdiction.

8 Education and Public Awareness

One of the strongest points emphasized during the webinar was the urgent need for digital education and public awareness.

Many individuals are unaware that:

- Data uploaded online may be used to train AI models
- Personal information may be harvested from public platforms
- Intellectual property may be inadvertently shared with AI tools

Speakers stressed that responsible use of AI begins with awareness.

Organizations such as LawDigits therefore play an important role in educating:

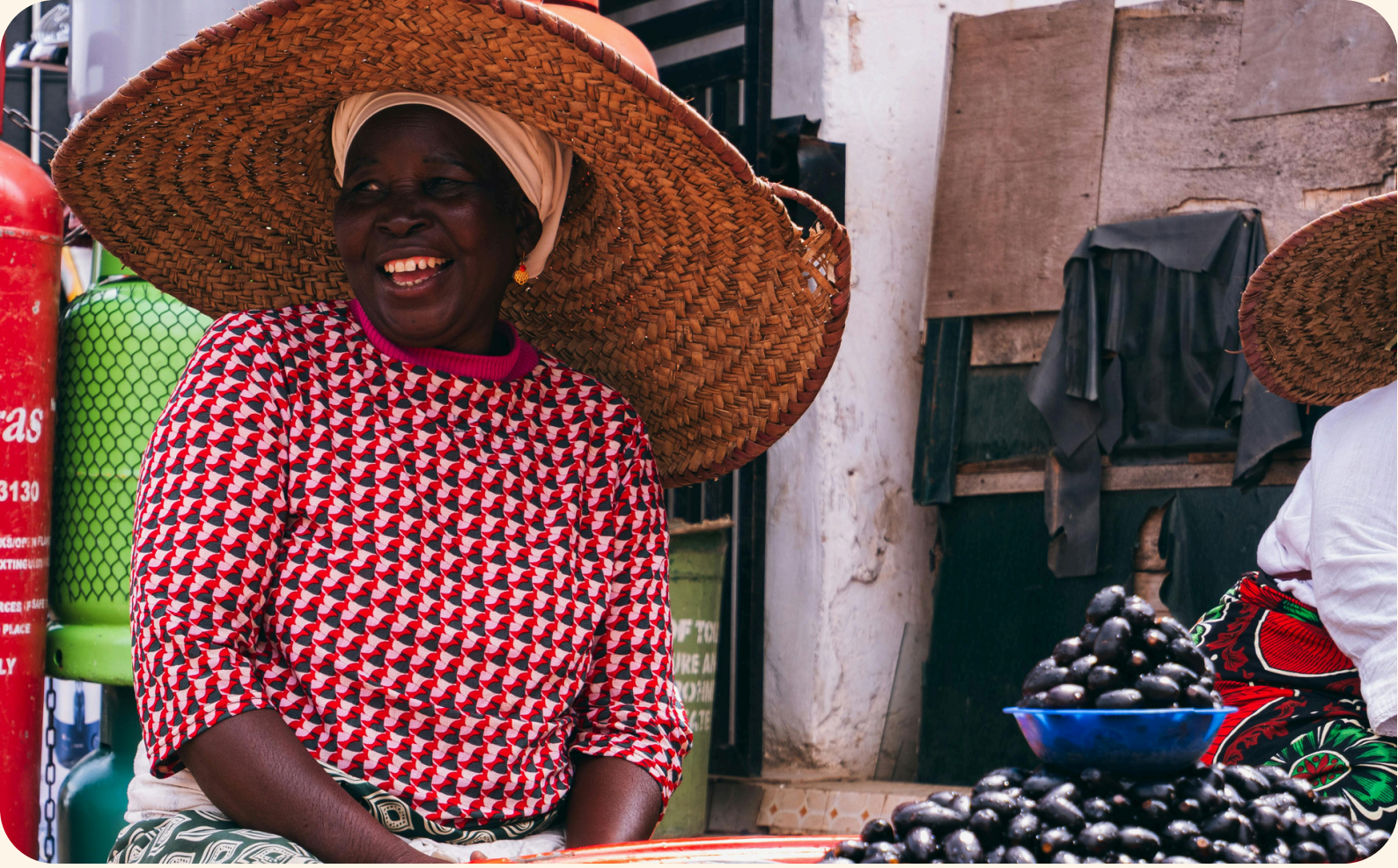
- Students
- Professionals
- Public institutions
- Businesses

Conclusion

The webinar provided an important platform for examining the legal, ethical, and governance implications of artificial intelligence in Nigeria. The discussion demonstrated that while AI offers enormous opportunities for innovation and development, it also introduces complex challenges concerning accountability, regulation, and technological sovereignty.

The panel concluded that addressing these challenges requires a multi-stakeholder approach involving governments, technology developers, regulators, legal professionals, and civil society.

Nigeria must work toward strengthening its regulatory capacity, technological infrastructure, and public awareness to ensure that AI technologies serve the public interest while minimizing harm.



Action Items and Recommendations

Based on the discussions during the webinar, the following key action points were identified:

Development of Domestic AI Infrastructure
Government and private sector stakeholders should invest in data centers, computing infrastructure, and research facilities to strengthen Nigeria's technological independence.

Strengthening AI Governance Frameworks
Regulators should develop clear guidelines for AI deployment, including sector-specific regulations for industries such as finance, healthcare, and law.

Promotion of Privacy by Design
AI developers and deployers should incorporate privacy-by-design and privacy-by-default principles into their systems.

Public Education and Capacity Building
Educational programs should be expanded to improve digital literacy, AI awareness, and data protection knowledgeacross society.

Encouraging Advocacy and Collective Legal Action
Civil society organizations should explore mechanisms for representative actions or class litigation to protect citizens from large-scale digital harms.

Responsible Corporate Use of AI
Organizations should adopt enterprise-grade AI solutions and ensure employee training on ethical and responsible AI usage.

Continued Multi-Stakeholder Engagement
LawDigits should continue organizing webinars, workshops, and public engagement initiatives to sustain conversations around responsible AI governance in Nigeria.