BIG TECH, BIG RISK: REGULATING INTERNATIONAL TECH GIANTS UNDER NIGERIA'S CYBER AND DATA PROTECTION LAWS

ONUCHUKWU, Victor Chinonye[1]

Abstract

This paper examines the regulatory challenges posed by international technology giants, commonly referred to as "Big Tech," operating in Nigeria, with a particular focus on data protection and cybersecurity. Companies such as Meta, Google, Apple, and Amazon collect and process vast amounts of personal data, creating significant risks including privacy breaches, unauthorised data use, market dominance, and potential threats to national security. Using a doctrinal research approach, the study critically analyses Nigeria's legal framework, including the Nigeria Data Protection Act (NDPA) 2023, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024), and related regulations from the Nigeria Data Protection Commission (NDPC), National Information Technology Development Agency (NITDA), and Nigerian Communications Commission (NCC). The analysis identifies gaps in enforcement, jurisdictional limitations, regulatory overlaps, and low public awareness, which constrain the effectiveness of existing laws in regulating foreign tech companies. The paper also examines the compliance obligations of Big Tech, encompassing data protection, cybersecurity, consumer protection, and digital taxation, and provides practical examples of non-compliance in Nigeria and beyond. Drawing on these findings, it proposes targeted legal and policy reforms, including mandatory data localisation for sensitive information, appointment of local regulatory representatives, enhanced enforcement powers, algorithmic transparency, and international cooperation. By addressing these challenges, Nigeria can establish a regulatory framework that ensures accountability of international tech companies while fostering innovation, economic growth, and the protection of users' rights. The study contributes to the discourse on digital governance in Africa, providing actionable insights for policymakers, regulators, and stakeholders as they navigate the balance between global digital engagement and local legal standards.

Keywords: Big Tech, Cybersecurity, Cross-Border Data Flow, Consumer Protection

1. Introduction

In recent years, international technology companies such as Meta, Google, Apple, and Amazon have expanded their operations across Africa, including Nigeria.[2] These companies collect and process large amounts of data from Nigerian users.[3] Their services influence communication, trade, education, and even politics. However, their activities raise concerns about data protection, user privacy, cybersecurity, and regulatory compliance. Nigeria has taken steps to regulate the digital space. The Nigeria Data Protection Act (NDPA) 2023 acts as a background for data protection in Nigeria. The Cybercrimes (Prohibition, Prevention) Act 2015 (as amended 2024) addresses various cyber threats.[4] These laws aim to protect users from misuse of their data and from cyber threats. They also try to hold both local and foreign companies accountable.

Regulating international tech giants is a difficult task. These companies, such as Google, Facebook, or Apple, are not based in Nigeria. They operate from countries like the United States or Ireland, but offer their services

[1] **ONUCHUKWU, Victor Chinonye, LL.B, BL, CIPP/E**, Data Protection Consultant and Partner at Cayan Technologies. Email:Onuchukwuvictor7@gmail.com; Phone Number: 08032010954

[2] Jaysim Hanspal, 'Google, Meta, Twitter…What tech giants bring to Africa', The African Report (10 January 2023) <https://www.theafricareport.com/272845/google-meta-twitter-what-tech-giants-bring-to-africa/> accessed on 7th June 2025

[3] Patrick Aloamaka, 'DATA PROTECTION AND PRIVACY CHALLENGES IN NIGERIA: LESSONS FROM OTHER JURISDICTIONS', Research Gate (July 2023) <https://www.researchgate.net/publication/373343733_DATA_PROTECTION_AND_PRIVACY_CHALLENGES_IN_NIGERIA_LESSONS_FROM_OTHER_JURISDICTIONS> accessed 7th June 2025

[4] …….. Act. s.21

in Nigeria through the internet. Because they are not physically present in Nigeria, it is hard for Nigerian authorities to fully control how they operate. To regulate them, Nigeria needs to create legal frameworks that can apply across borders. This is not easy, because laws made in Nigeria may not have direct power over companies that are outside the country. Also, these tech companies have a lot of money and legal support. If Nigeria tries to enforce its laws against them, these companies may take legal steps to resist or delay action. This makes enforcement slow, expensive, and uncertain. At the same time, Nigeria must be careful not to break international agreements it has signed.[5] These agreements may protect foreign companies from unfair treatment. There is also the possibility that if Nigeria is too aggressive in applying its laws, it might scare away other investors. Tech companies may feel Nigeria is too risky or difficult to do business in, and this could reduce investment in Nigeria's growing tech sector. This paper examines the challenges and prospects of regulating international tech companies under Nigeria's cyber and data protection laws. While Nigeria's legal framework - anchored on the NDPA 2023, Cybercrimes Act, Finance Acts, and regulatory directives - formally empowers it to regulate international Big Tech within its digital space, enforcement is crippled by structural and practical barriers such as limited jurisdiction, weak institutional capacity, regulatory overlap, and low public awareness. Without urgent reforms and targeted capacity building, the framework will remain ineffective in practice.

2. Conceptual Clarifications

Clear definitions are important in legal writing, especially in fast-changing areas like technology law. Defining these terms clearly will help ensure a focused and consistent analysis of how Nigeria responds to regulatory challenges posed by major international tech companies. 'Big Tech' refers to the largest and most influential technology companies that provide digital platforms, online services, cloud infrastructure, and data-driven technologies.[6] Examples include Google (Alphabet), Meta (Facebook), Amazon, Apple, and Microsoft. These companies operate across borders and have a global user base. 'Data Protection', under the NDPA 2023, refers to the legal and institutional measures aimed at ensuring the privacy, security, and lawful processing of personal data.[7] Section 65 of the NDPA defines 'personal data' as any information relating to an identified or identifiable natural person. The law regulates how data is collected, stored, used, and shared. It creates obligations for data controllers and processors, including foreign entities that collect data from Nigerian residents.[8] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 governs cybersecurity in Nigeria. The Act defines cybercrime broadly and includes offences such as hacking, identity theft, cyberstalking, and data interference.[9] Cybersecurity under this law refers to the protection of computer systems, networks, and electronic communications from unauthorised access, attack, or damage. It also includes provisions for securing critical national information infrastructure and protecting digital systems from exploitation.[10]

3. Explanation of Jurisdictional and Cross-Border Data Issues:

Jurisdiction refers to the legal authority of a country to regulate persons, property, or conduct.[11] A major challenge in regulating Big Tech is the question of whether Nigerian authorities can exercise jurisdiction over companies that do not have a physical office or staff in Nigeria but collect data from Nigerian users. The NDPA 2023 attempts to address this by applying to data controllers and processors outside Nigeria if they process the personal data of individuals located in Nigeria.[12] Cross-border data issues arise when

[5] Jide Nzelibe, 'The Breakdown of International Treaties', (2017) *Notre Dame L. Rev*. 93 1173

[6] Siddhesh Shinde, 'What Companies Fall Under Big Tech? How Do You Land a Job With Them?', Emeritus (21 February 2023) <https://emeritus.org/blog/technology-big-tech/> accessed on 7th June 2025

[7] NDPA s. 65

[8] NDPA. Part V

[9] NDPA. Part III

[10] NDPA. ss. 5 and 6

[11] Oputa JSC in *Sanusi v. Olalere* (1988) NWLR (Pt.69) 207 thus, 'Jurisdiction is the legal authority, the extent of the power given to a Court by the law or statute establishing the said Court. This jurisdiction may be limited or unlimited. It may be limited either locally, that is, in terms of the geographical area over which the Court's jurisdiction may extend.'

[12] NDPA. s. 2(2)

personal data is transferred from Nigeria to servers or entities outside the country.[13] This creates risks of loss of control, weaker protection standards, and difficulty in enforcement. The NDPA includes provisions that restrict such transfers unless the receiving country ensures an adequate level of protection or other safeguards are in place.[14] These conceptual clarifications form the basis for understanding how Nigeria regulates Big Tech under its current legal framework.

4.0 Legal Framework Governing Big Tech in Nigeria

Nigeria's legal framework for regulating international tech giants is primarily built upon the Cybercrimes Act (most recently amended in 2024) and the Nigeria Data Protection Act (NDPA) 2023, along with subsidiary regulations and guidelines from bodies like the Nigeria Data Protection Commission (NDPC). The Cybercrimes Act addresses offenses such as hacking, data interference, and cyber fraud, imposing penalties and requiring reporting of cyber threats. Crucially, the NDPA establishes a comprehensive data protection regime, outlining principles like data minimization and purpose limitation, granting data subjects rights (e.g., right to be forgotten, data portability), and mandating data breach notifications within 72 hours. These laws, while significant strides, face unique challenges in their application to 'Big Tech' particularly concerning their extraterritorial reach, the complexity of cross-border data flows, and the practicalities of enforcement against entities often without a physical presence or easily identifiable assets within Nigeria.

4.1 Applicable laws and regulations in Nigeria

Several laws and regulations apply to the regulation of international technology companies in Nigeria. These legal instruments govern data protection, cybersecurity, digital services, and consumer rights.

4.1.1 Constitution of the Federal Republic of Nigeria 1999 (as amended)

Section 37 guarantees the right to privacy, including the privacy of homes, correspondence, telephone conversations, and telegraphic communications. This constitutional right forms the foundation for data protection and limits to state or corporate surveillance. These laws and regulations form the legal environment within which Nigeria attempts to regulate the activities of international technology companies. They provide the basis for enforcement actions, compliance expectations, and protection of Nigerian users in the digital space.

4.1.2 Nigeria Data Protection Act (NDPA) 2023

This is the main law governing the collection, processing, storage, and transfer of personal data in Nigeria. Key features include:

- It establishes the Nigeria Data Protection Commission (NDPC) as the primary regulator.[15]
- It applies to both local and foreign data controllers or processors who handle the personal data of individuals located in Nigeria.[16]
- It sets out principles of data processing such as lawfulness, fairness, transparency, purpose limitation, and data minimisation.[17]
- It provides for data subject rights, including the right to access, rectification, erasure, and objection.[18]
- It regulates cross-border data transfers and prescribes penalties for non-compliance.[19]

4.1.3 Cybercrimes (Prohibition, Prevention, etc.) Act 2015

This law addresses offences committed through or against computer systems and digital platforms. Relevant provisions include:

[13] NDPA. Part VIII
[14] NDPA ss. 41 – 43
[15] NDPA. s 4
[16] NDPA. s 2
[17] NDPA. Part V
[18] NDPA. Part VI
[19] NDPA. Part VIII

- Prohibition of hacking, system interference, and unlawful interception of data.[20]
- Regulation of electronic transactions and e-banking.[21]
- Protection of critical national information infrastructure.[22]
- Establishment of procedures for investigation, prosecution, and international cooperation on cybercrime matters.[23]

4.1.4 Nigeria Communications Commission (NCC) Regulations

The NCC regulates telecom companies and digital service providers. Key regulations include:
Consumer Code of Practice Regulations 2007 – which ensures consumer rights in digital and telecom services. Registration of Telephone Subscribers Regulations – which requires SIM card registration and supports digital identity tracking. NCC also issues directives to service providers on data handling, quality of service, and lawful interception.

4.1.5 Freedom of Information (FOI) Act 2011

This law grants citizens the right to access public records and information. It includes provisions that protect certain categories of personal and sensitive information. While it promotes transparency, it also supports data privacy by restricting access to personal data unless legally justified.

4.1.6 Federal Competition and Consumer Protection Act (FCCPA) 2018

The Federal Competition and Consumer Protection Act (FCCPA) 2018 plays a supporting role in the regulation of international tech giants in Nigeria, especially in areas where their conduct affects market competition and consumer rights. Big Tech companies like Google, Meta, and Apple engage in practices that limit competition - such as favouring their own products in search results or app stores.[24] The FCCPA prohibits abuse of dominant market position and restrictive agreements.[25] It gives the Federal Competition and Consumer Protection Commission (FCCPC) the power to investigate and sanction such behaviour.[26] As an example, if a Big Tech company restricts Nigerian developers from fairly accessing its platform, the FCCPC can intervene. In addendum, the FCCPA protects consumers from unfair trade practices, misleading information, and exploitation.[27] This is relevant where Big Tech companies collect or use Nigerian consumers' data without transparency or consent, especially if such use causes harm or violates privacy rights.

4.1.7 Finance Act 2021 (as amended 2023)

The Finance Act 2023 introduced several important provisions to help Nigeria tax the digital economy more effectively. These changes directly affect international tech companies and users of digital platforms, including those involved in cryptocurrency, e-commerce, and online services. One of the key changes is the introduction of Capital Gains Tax (CGT) on digital assets.[28] Before the Act, digital assets like cryptocurrencies were not clearly covered by Nigerian tax laws. Now, when a person sells or disposes of a digital asset and makes a profit, that profit is subject to a 10% capital gains tax. The Act also allows losses from digital asset transactions to be offset against future gains for up to five years.[29] This means that if someone loses money on a cryptocurrency sale, they can reduce future taxable gains by the amount lost. The Act also made changes to the Value Added Tax (VAT) system to ensure that foreign companies providing

[20] Cybercrimes (Prohibition, Prevention, etc.) Act 2015. s. 8
[21] ibid. s 14
[22] ibid. s. 5
[23] ibid. Part VI
[24] Megan Case, 'Google, Big Data, & Antitrust', Del. J. Corp. L. 46 (2021): 189
[25] FCCPA. s. 2
[26] FCCPA. s. 17
[27] ibid.
[28] Finance Act 2023. s. 2
[29] Finance Act 2023. s. 3

digital services to Nigerian consumers are brought into the tax net.[30] Under the new rules, non-resident suppliers of digital goods and services are required to register with the Federal Inland Revenue Service (FIRS) or appoint a local agent.[31] This allows the Nigerian government to collect VAT from purchases made through foreign online platforms. For example, if a Nigerian customer buys an app from an international app store or pays for a subscription to a streaming service, VAT is now chargeable on that transaction.

Another important aspect of digital taxation, although introduced earlier in the Finance Act 2020, is the concept of Significant Economic Presence (SEP).[32] This provision allows Nigeria to tax foreign tech companies that earn more than ₦25 million annually from Nigerian users, even if they have no physical office in Nigeria. The SEP rules target digital advertising, e-commerce, and online services provided from abroad. When combined with the new Finance Act 2023 provisions, the SEP framework helps Nigeria collect taxes from foreign companies that benefit from the Nigerian market without being locally established.

5. 0 Compliance Obligations of Big Tech Companies Operating in Nigeria

International technology companies that offer digital services to users in Nigeria have several legal obligations under Nigerian law. These obligations apply even if the company is not physically present in Nigeria, as long as it collects or processes the personal data of Nigerian residents or offers digital services within Nigeria's digital space.

Below are the key compliance obligations:

5.1 Data Protection Obligations (Under the NDPA 2023)

Big Tech companies must ensure that personal data is processed on a lawful basis.[33] This includes consent, performance of a contract, legal obligation, protection of vital interests, public interest, or legitimate interest.[34] Also, they must inform users, in clear language, about how their data will be used, who it may be shared with, and how long it will be stored.[35] Companies must provide mechanisms for users to exercise their rights. These rights include access to their data, correction of inaccurate data, erasure of data (the 'right to be forgotten'), and objection to data processing.[36] A Data Protection Officer must be appointed where required, especially if the company engages in large-scale data processing.[37] Data may only be transferred outside Nigeria if the recipient country provides adequate protection or if legal safeguards (such as standard contractual clauses) are in place.[38]

Companies are expected to submit annual data protection audit reports to the Nigeria Data Protection Commission (NDPC).[39]

5.2 Cybersecurity Obligations (Under the Cybercrimes Act 2015)

Companies should implement adequate technical and organisational measures to protect systems from cyberattacks, unauthorised access, and data breaches.[40] In the event of a cyber breach, companies must notify the National Computer Emergency Response Team (NCERT) or relevant authorities promptly.[41] Companies must respond to lawful requests from Nigerian law enforcement agencies for access to electronic records in the investigation of cybercrimes.[42]

[30] VAT Act. s. 10 (1)
[31] ibid.
[32] CITA. s.13 (2)
[33] NDPA. s 14
[34] NDPA. s 25
[35] NDPA. s 26
[36] NDPA. s. 34
[37] NDPA. s. 32
[38] NDPA. ss. 41-43
[39] NDPA. s. 33
[40] General Data Protection Regulation (GDPR). Art. 32
[41] Cybercrimes Act 2025. s. 21
[42] ibid. s. 46

5.3 Registration and Regulatory Engagement

Depending on the nature of services offered (e.g., digital payments, cloud services, telecom services), companies may need to register with the National Information Technology Development Agency (NITDA), Nigeria Data Protection Commission (NDPC), or Nigerian Communications Commission (NCC).

5.4 Consumer Protection Obligations

Under NCC and general consumer protection principles, companies must avoid deceptive practices. They must ensure that terms of service and privacy policies are accessible and fair. Platforms like social media companies must have policies for managing harmful content, misinformation, or abuse. They will be held accountable for failing to act on complaints or remove unlawful content, especially in sensitive periods such as elections.

5.5 Tax and Economic Compliance (Emerging Requirement)

Nigeria has introduced digital tax provisions under the Finance Act 2023. These obligations reflect Nigeria's attempt to create a responsible digital economy. Big Tech companies must ensure ongoing compliance, maintain engagement with Nigerian regulators, and adapt their internal policies and systems to meet the legal requirements. Failure to comply will lead to appropriate sanctions, fines, service restrictions, or reputational damage.

6.0 Practical examples of how Big Tech companies have failed to comply with local laws:

This section contains practical examples of how Big Tech companies have failed to comply with local laws and the reverberating consequences:

6.1 Meta (Facebook) – Data Privacy Breaches

Meta has faced multiple data privacy issues globally. In 2019, it was fined $5 billion by the U.S. Federal Trade Commission (FTC) for violating user privacy rules in the Cambridge Analytica scandal.[43] Cambridge Analytica was also accused of interfering in Nigeria's 2015 elections by harvesting Facebook user data.[44] This incident shows how foreign tech companies can misuse Nigerian users' data without local accountability.

6.2 Google – Non-compliance with Antitrust and Data Rules

In 2021, the French competition authority fined Google €220 million for abusing its market dominance in digital advertising.[45] In India, the Competition Commission of India fined Google over $160 million for anti-competitive practices related to Android devices.[46] Google operates a dominant position in search and mobile operating systems (Android) in Nigeria, but there is limited local oversight. Similar anti-competitive concerns could arise in Nigeria without clear enforcement of competition and data protection laws.

6.3 Twitter – Banned in Nigeria (2021)

The Nigerian government banned Twitter in June 2021 after it deleted a tweet by the President.[47] The government accused Twitter of undermining Nigeria's sovereignty and failing to register locally or pay taxes.

---

[43] Federal Trade Commission (24 July 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>; accessed on 9th June 2025

[44] Channels Television, <https://www.channelstv.com/2018/04/01/fg-investigates-cambridge-analyticas-alleged-interference-in-2015-elections/amp/>; accessed on 9th June 2025

[45] 'French regulator fines Google €220 million for abusing dominant market position', France24 (07/06/2021) <https://www.france24.com/en/business/20210607-french-regulator-fines-google-%E2%82%AC220-million-over-advertising-practices>; accessed on 9th June 2025

[46] 'Google: India tribunal upholds $160m fine on company', BBC (30 March 2023) <https://www.bbc.com/news/world-asia-india-65120697>; accessed on 9th June 2025

[47] Emmanuel Akinwotu, 'Nigeria suspends Twitter access after president's tweet was deleted', Guardian (4th June 2021) <https://www.theguardian.com/world/2021/jun/04/nigeria-suspends-twitter-after-presidents-tweet-was-deleted>; accessed on 9th June 2025

Twitter was accused of not complying with Nigeria's requirements for a physical presence and registration as a legal entity. The ban lasted seven months. Twitter agreed to open a local office, register with the Corporate Affairs Commission, and pay applicable taxes.

6.4 TikTok – Data Harvesting and Children's Privacy

In 2023, the U.K. fined TikTok £12.7 million for illegally processing the data of children under 13 without parental consent.[48] TikTok has a large Nigerian user base, including minors. If similar practices occur in Nigeria, they would violate the Nigeria Data Protection Law and the Child's Rights Act (CRA),[49] but enforcement remains weak due to lack of local control over TikTok. These examples show that Big Tech often fails to comply with local laws unless pressured. Data protection, tax compliance, and local presence are common issues.

7. Key Challenges in Regulating Big Tech in Nigeria

Regulating international technology companies in Nigeria is a complex task. Although legal frameworks exist, several practical challenges limit the ability of Nigerian authorities to effectively regulate Big Tech companies. These challenges are outlined below:

1. Many Big Tech companies operate in Nigeria's digital space without having an office, staff, or data center within the country.[50] This makes it difficult to serve legal notices, carry out investigations, or enforce penalties.
2. Nigerian laws apply within Nigeria. However, Big Tech companies are headquartered in other countries and may argue that foreign laws govern their operations.[51] This raises issues about the reach of Nigerian law and whether foreign courts will cooperate with Nigerian regulators. As an example, if a data breach occurs on a platform operated by a company in the United States, Nigerian regulators may have limited means to compel that company to take corrective action or to pay fines.
3. Regulatory bodies such as the Nigeria Data Protection Commission (NDPC) and the National Information Technology Development Agency (NITDA) may lack the financial, technical, and human resources needed to monitor and enforce compliance by large foreign companies. Advanced data analytics, artificial intelligence, and algorithmic decisions used by Big Tech companies require strong technical knowledge to audit and regulate. Personal data collected from Nigerians is often stored on servers outside Nigeria. This reduces control over how data is processed or protected, especially if the foreign country has weak data protection laws.
4. Big Tech platforms contribute to the digital economy. They provide advertising, payments, communications, and jobs. Strict enforcement is often seen as a threat to economic growth, making regulators cautious. As an example, regulatory actions against a major platform like YouTube or Facebook will affect small businesses that rely on them for marketing and sales.
5. Also, due to multiple regulators, agencies such as NDPC, NITDA, NCC, and others issue overlapping guidelines. This can create confusion about which rules apply and who is responsible for enforcement.
6. Many users are unaware of their rights under data protection and cybersecurity laws. This reduces pressure on companies to comply and weakens the role of public accountability. Few NGOs or watchdogs focus on tech accountability in Nigeria. This limits the number of independent actors pushing for compliance and transparency.

---

[48] 'ICO fines TikTok £12.7 million for misusing children's data', Information Commissioners Officer (4th April 2023) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/>; accessed on 9th June 2025

[49] CRA s. 8

[50] John Ameh, 'Senate wants Facebook, X, Whatsapp, others to open physical offices in Nigeria', Tribune Online (3 months ago) <https://www.google.com/amp/s/tribuneonlineng.com/senate-wants-facebook-x-whatsapp-others-to-open-physical-offices-in-nigeria/amp/> accessed on 7th May 2025

[51] Parisa Danesh, Amir Hossein Yazdani, and Leyla Rahimi, 'Transnational Governance of the Digital Economy: Legal Approaches to Regulating Big Tech Companies and Ensuring Global Compliance', (2022) 1 Legal Studies in Digital Age 1, 27 – 38

8. Policy and Legal Reform Recommendations

Nigeria must address the regulatory mismatch between the influence of international tech giants and the country's current legal capacity to control their operations. The Nigeria Data Protection Act 2023 (NDPA) and the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 are foundational, but both require targeted reforms to deal with global digital power.

First, Nigeria should establish a mandatory data localisation framework for certain categories of sensitive personal data. While current laws encourage data sovereignty, they stop short of requiring tech giants to store or process Nigerian data within Nigeria. A localisation requirement - especially for critical infrastructure, financial, and biometric data - would limit offshore abuse and improve enforcement reach.[52]

Second, the country should create an accountability mechanism for foreign data controllers. The NDPA should be amended to mandate the appointment of local data protection representatives by all foreign platforms that collect or process the personal data of Nigerians. This would give the Nigeria Data Protection Commission (NDPC) a physical point of contact for enforcement, including fines, investigations, or service of legal documents.

Third, Nigeria needs to upgrade enforcement powers and funding for the NDPC. At present, the Commission's power is limited by administrative reach and technical capacity.[53] It should be empowered to enter into enforcement partnerships with global regulators (such as the EU or UK ICO), and to impose tiered fines based on global turnover - similar to the EU's GDPR regime. This would deter noncompliance by large players like Meta, Google, or X (formerly Twitter).

Fourth, there should be a clear framework for algorithmic accountability and AI regulation. Nigeria's current cyber and data protection laws are silent on how Big Tech deploys algorithms to manipulate user behaviour, curate content, or target ads. A new regulation - modelled on international AI principles - should require transparency reports, opt-outs from profiling, and impact assessments where automated systems affect users' rights.

Fifth, the Cybercrimes Act should be reviewed to clarify liability for platform-based harm, including misinformation, electoral manipulation, and abuse of local laws. Nigeria should hold platforms to a 'duty of care' standard for user-generated content, with clear notice-and-takedown obligations. This ensures that freedom of expression is balanced with protection against digital harm.

Finally, Nigeria must develop a cross-border cooperation policy that allows it to enter into mutual legal assistance arrangements with other jurisdictions. This is necessary for digital forensics, cross-border investigations, and recovery of data or assets in global cybercrime cases. Big Tech regulation is a global challenge; Nigeria must not act alone.

To improve regulation of Big Tech companies in Nigeria, several policy and legal reforms are needed. These reforms should address current gaps, strengthen enforcement, and promote cooperation with international partners.

- Amending laws like the NDPA to clearly state that Nigerian regulators have authority over foreign companies processing Nigerian data, regardless of physical presence. This reduces ambiguity about jurisdiction. Requiring foreign digital companies to appoint a local representative or establish a legal entity in Nigeria for regulatory and legal accountability.

[52] John Selby, 'Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?', (2017) 25(3) *International Journal of Law and Information Technology*, 213 – 232

[53] I. Juma & B. Faturoti, 'Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice', (2025) *International Review of Law, Computers & Technology*, 1 – 26, https://doi.org/10.1080/13600869.2025.2506918

- More budget and resources to the Nigeria Data Protection Commission (NDPC), NITDA, and other relevant agencies to improve staffing, training, and technology.
- Invest in training regulatory personnel in areas such as data science, cybersecurity, and digital forensics to better understand and monitor Big Tech operations.
- Coordination between NDPC, NITDA, NCC, and other agencies to create clear, consistent guidelines on data protection and cybersecurity that apply to all digital service providers.
- Issue specific rules on data transfers, consent mechanisms, data breach notifications, and platform responsibilities, to reduce loopholes.
- Establish formal agreements with countries where Big Tech companies are based to facilitate cooperation on investigations, data sharing, and enforcement actions.
- Participate actively in African Union or ECOWAS initiatives to develop regional standards and cooperation mechanisms on data protection.
- Require Big Tech companies to publish transparency reports detailing data requests, content moderation policies, and data breaches affecting Nigerian users.
- Launch public awareness campaigns to educate Nigerian citizens on their data protection rights and how to exercise them.
- Create accessible mechanisms for users to lodge complaints and resolve disputes with Big Tech companies.

9. Conclusion

Regulating Big Tech companies in Nigeria presents challenges due to jurisdictional limits, cross-border data flows, and enforcement difficulties. However, Nigeria's existing legal framework, including the Nigeria Data Protection Act and the Cybercrimes Act, provides a foundation for protecting user data and promoting cybersecurity. To effectively regulate international tech giants, Nigeria must strengthen its laws, improve regulatory capacity, and enhance cooperation with foreign jurisdictions. Clear rules on data protection, local representation, and transparency will hold Big Tech accountable while supporting economic growth.