

A CRITICAL ANALYSIS OF NIGERIA'S CROSS-BORDER E-COMMERCE, DATA PRIVACY AND CYBERSECURITY LAWS AGAINST COMPARATIVE BEST PRACTICE

Oluwatosin Rebecca Folagbade*

Abstract

Nigeria's digital economy has expanded faster than the statutory framework meant to govern it. Four bodies of law bear directly on cross-border digital trade: the Nigeria Data Protection Act 2023 (NDPA), regulating international personal-data transfers; the Cybercrimes (Prohibition, Prevention, etc) Act 2015 as amended in 2024, addressing the security of computer systems and electronic transactions; the Electronic Transactions Act 2023 and Federal Competition and Consumer Protection Act 2018 (FCCPA), governing online contract formation and consumer protection; and the Central Bank of Nigeria's payment-system regulation, governing the infrastructure over which most cross-border e-commerce clears. Each was drafted and is largely enforced without sustained reference to the others, and without a shared institutional mechanism for resolving overlaps. This article undertakes a gap analysis of that arrangement, tested against comparative practice in the European Union, South Africa, Kenya and Singapore, and grounded in Nigerian judicial authority, regulatory guidance and enforcement practice. It identifies five persistent shortfalls: unresolved ambiguity in the NDPA's adequacy-determination mechanism; the absence of any Nigerian adequacy decision four years after the Act's commencement; a widening implementation gap between Nigeria's 2024 ratification of the AfCFTA Digital Trade Protocol and its domestic statutes; the lack of a cross-border consumer dispute-resolution channel; and a documented jurisdictional contest between Nigeria's data, competition and payment

* LL.B(Hons), B.L, LLM, PhD Candidate, Department of Business Law, Faculty of Law, University of Ilorin, Nigeria. Email: folagbade.or@unilorin.edu.ng,

regulators leaving digital lending and payment platforms without settled regulatory ownership. These are not defects internal to any one statute but structural gaps between statutes and institutions, requiring a single legislative framework rather than further piecemeal amendment.

Keywords: cross-border data transfer; cybersecurity law; e-commerce regulation; AfCFTA Digital Trade Protocol; payment systems regulation.

I. INTRODUCTION

Nigeria's digital economy is now a significant contributor to national output, and its growth is increasingly cross-border in character, spanning warehousing, payment clearing and data storage arrangements that now routinely sit outside the country. The legal instruments that were meant to govern this activity, however, were built at different times, by different drafters, for different immediate purposes. The Nigeria Data Protection Act 2023 answers to a data-privacy agenda shaped substantially by the General Data Protection Regulation.¹ The Cybercrimes Act 2015 and its 2024 amendment, answer to a security and law-enforcement agenda shaped by the Budapest Convention on Cybercrime.² The Electronic Transactions Act 2023 and the FCCPA 2018 answer to a commercial and consumer-protection agenda with roots in the UNCITRAL Model Law on Electronic Commerce.³ None of the three was drafted with express regard to how a single cross-border transaction would move through all three regimes, and through the Central Bank of Nigeria's separate payment-system rules, at once.

¹Regulation (EU) 2016/679 (General Data Protection Regulation).

²Council of Europe, Convention on Cybercrime (Budapest Convention) 2001, ETS No 185.

³United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce 1996.

This article asks a narrower question than 'what should Nigeria's digital economy law look like': it asks where, specifically, the current arrangement of statutes, regulatory directives and case law fails to cover, or fails to coordinate the cross-border movement of data, money and goods.

The methodology adopted is doctrinal and comparative. The Nigerian statutes and their implementing directives are read against the primary legislative text of the four comparator jurisdictions, against Nigerian judicial authority interpreting those statutes and their predecessors, and against recent regulatory and practitioner commentary. The comparative jurisdictions were chosen for contrast: the European Union supplies the doctrinal template Nigeria's own adequacy mechanism follows; Kenya supplies a functioning African Union regional example operating under the same AfCFTA obligations as Nigeria, adopted in February 2024;⁴ and Singapore supplies a working alternative to country-by-country adequacy listing.

II. DISCUSSION

A. Nigeria's Current Legal Regime

1. Constitutional Foundation and Judicial Recognition

Nigeria's data protection regime has constitutional roots that predate the NDPA. Section 37 of the 1999 Constitution guarantees citizens the right to their private and family life,⁵ and the Court of Appeal's 2021 decision in *Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission* held that this right encompasses data protection.⁶ The Federal High Court had earlier

⁴International Institute for Sustainable Development, 'The AfCFTA Digital Protocol' (30 October 2024) <<https://www.iisd.org/articles/policy-analysis/afcfta-digital-protocol>>.

⁵Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

⁶*Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission* (2021) LPELR-55623(CA).

reached a similar result in *Emerging Markets Telecommunication Services v Godfrey Nya Eneye*, awarding damages for a section 37 breach.⁷ Courts have also required exhaustion of administrative redress before court action,⁸ and a further decision in *Olumide Babalola v Soko Lending Company Limited* addressed unlawful data-driven debt-recovery practices, foreshadowing the digital-lending dispute examined below.⁹ The Cybercrimes Act's core offences survived early constitutional challenge in *Paradigm Initiative v Attorney General of the Federation* and rest on settled footing.¹⁰¹¹

2. Data Privacy: The Nigeria Data Protection Act 2023

The NDPA repealed the Nigeria Data Protection Regulation 2019, giving Nigeria's data protection regime the force of primary legislation.¹² Sections 41 to 43 govern cross-border transfers: section 41 bars transfer outside Nigeria absent a statutory basis;¹³ section 42 supplies the primary basis, adequacy, empowering the Nigeria Data Protection Commission to assess whether a recipient jurisdiction or transfer mechanism affords comparable protection;¹⁴ and section 43 supplies derogations including consent, contractual necessity and public interest.¹⁵ Read with the Commission's General Application and

⁷*Emerging Markets Telecommunication Services v Godfrey Nya Eneye* (2018) LPELR-46193(CA).

⁸*Incorporated Trustees of Digital Rights Lawyers Initiative v Unity Bank Plc*, discussed in Chukwuka (2022) 12 International Data Privacy Law 44.

⁹*Olumide Babalola v Soko Lending Company Limited* (Federal High Court, 17 February 2023, Ashade J), noted in Chukwuka (n 9).

¹⁰*The Incorporated Trustees of Paradigm Initiative for Information Technology Development v Attorney General of the Federation* (CA/L/556/2017, 1 June 2018).

¹¹*Cybercrimes (Prohibition, Prevention, etc.) Act 2015*, ss 24 and 38, upheld as constitutional in *Paradigm Initiative* (n 11).

¹²*Nigeria Data Protection Regulation 2019* (repealed); INPLP, 'Salient Features of Nigeria's Novel NDPA 2023' (2023).

¹³*Nigeria Data Protection Act 2023*, s 41(1).

¹⁴*Nigeria Data Protection Act 2023*, s 42.

¹⁵*Nigeria Data Protection Act 2023*, s 43.

Implementation Directive 2025, the effect is a three-tier structure of adequacy, approved instruments, and residual derogations,¹⁶ though the Directive took effect only in September 2025, two years after the Act itself commenced.¹⁷ How rigorously such determinations should be policed is not new: under the NDPA's predecessor regime, Ikigai Innovation Initiative successfully challenged NITDA's country 'whitelist' as including jurisdictions lacking any data protection law,¹⁸¹⁹ and the transfer mechanisms struck down in that case have since been reintroduced on a statutory footing.²⁰ The episode shows Nigerian courts are willing to scrutinise the substance of an adequacy determination, a precedent the Commission has not yet been tested against under section 42. Separately, the Act's threshold definition of a controller or processor 'of major importance', fixed at more than 200 data subjects in any six-month period,²¹ triggers heavier obligations including mandatory registration²² and appointment of a Data Protection Officer,²³ enforced through tiered administrative fines.²⁴ None of this machinery, however, addresses the adequacy question directly.

¹⁶Nigeria Data Protection Commission, General Application and Implementation Directive 2025, art 45 and sch 5.

¹⁷The GAID took effect 19 September 2025: Cookie Yes, 'NDPA 2023: Guide for Businesses in 2025' (2025).

¹⁸Incorporated Trustees of Ikigai Innovation Initiative v National Information Technology Development Agency, Suit No FHC/ABJ/CS/1246/2022 (2023).

¹⁹Ikigai Innovation Initiative, 'Federal High Court Nullifies Part of the Adequacy of the "Whitelist" on International Data Transfer' (2025).

²⁰TechHive Advisory, 'Changing Trend in International Data Transfer in Nigeria' (2025), noting Ikigai's struck-down mechanisms have since been re-introduced.

²¹Nigeria Data Protection Act 2023, s 5(d); NDPC, 'Guidance Notice: Registration of Data Controllers and Processors of Major Importance'.

²²Nigeria Data Protection Act 2023, s 65; AELEX, 'Highlights of the Data Protection Act, 2023'.

²³Gelias, 'Nigeria Data Protection Act, 2023: A Review', identifying six lawful bases including consent, contractual necessity and legitimate interest.

²⁴Regulations.AI, 'Nigeria Data Protection Act (NDPA)' (2026), setting fines up to NGN10,000,000 or 2% of gross revenue.

3. Cybersecurity: The Cybercrimes Act 2015 and its 2024 Amendment

The Cybercrimes (Prohibition, Prevention, etc) Act 2015 was Nigeria's first comprehensive cybercrime statute. Nine years of enforcement experience and Nigeria's 2022 accession to the Budapest Convention prompted the 2024 Amendment,²⁵ which introduced a 72-hour incident-reporting deadline, mandated sector-specific Computer Emergency Response Teams, tightened Know-Your-Customer obligations, and created a National Cybersecurity Fund financed by a transaction levy.^{26,27} The amendment's most significant feature for present purposes is its express cross-reference to the NDPA: service providers must now store and secure user data for two years consistently with both statutes.²⁸ This is the only point of statutory contact between Nigeria's cybersecurity and data-privacy regimes, and a narrow one. The Fund's 0.5% levy, introduced by Central Bank circular,²⁹ was itself suspended within three months following public objection.³⁰

4. Cross-Border E-Commerce: The Electronic Transactions Act 2023 and the FCCPA 2018

²⁵Nigeria acceded to the Budapest Convention in 2022: LIRAD, 'Nigeria's Cybercrime (Amendment) Act 2024' (2025).

²⁶Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, signed into law 28 February 2024.

²⁷AB Legal Practitioners, 'A Review of the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024' (2025).

²⁸Record of Law, 'Legal Challenges in Combatting Cybercrime in Nigeria' (2025), detailing the 72-hour incident-reporting deadline.

²⁹AB Legal Practitioners (n 35), on the Amendment Act's two-year data storage requirement.

³⁰TechHive Advisory, 'Nigeria Cybercrimes Act Amendment' (2025), on the 0.5% Cybersecurity Fund levy under s 44.

The Electronic Transactions Act 2023 is the most directly relevant statute governing online contract formation, electronic signatures, and baseline disclosure; section 16(1) requires e-commerce businesses to disclose full pricing and product information.³¹ The FCCPA 2018 supplies the general consumer-protection backdrop, establishing the Federal Competition and Consumer Protection Commission.³² Nigerian scholarship converges on a common diagnosis: the FCCPA was not written with the digital economy in mind, and neither statute equips the Commission with an international cooperation or dispute-resolution mechanism.³³ Where a platform is domiciled outside Nigeria, a consumer's avenues for redress remain limited, a gap recent comparative work traces to the absence of any cross-border enforcement channel comparable to the WTO's dispute settlement system.³⁴

5. Payment Infrastructure: Central Bank of Nigeria Regulation and the Digital Lending Dispute

A fourth, easily overlooked layer governs the infrastructure through which cross-border transactions clear. The Central Bank's 2020 circular established licensing categories for non-bank payment participants,³⁵ with capital requirements and separate IT and data-protection obligations for licence applicants,³⁶ and its Open Banking Framework and 2023 Operational Guidelines layer a further data-sharing regime requiring API providers and consumers to meet

³¹*ibid*, on the House of Representatives' direction to the Central Bank of Nigeria to suspend implementation of the levy.

³²*ibid*, on the CBN's revised circular of 17 May 2024 retracting the levy directive.

³³Nigerian Communications Act 2003.

³⁴Abiodun Amuda-Kannike (2024) *Journal of Contemporary Private Law*.

³⁵Central Bank of Nigeria, 'CBN License Categorization for Nigeria Payment System' (Circular, 9 December 2020).

³⁶Legal 500, 'Fintech Licenses Required for Operation in Nigeria'.

independent consent and security obligations³⁷³⁸ that do not cross-reference the NDPA. Cross-border flows attract further Central Bank regulation: the 2024 Reviewed Guidelines on International Money Transfer Services restrict operator licensing to non-bank, non-fintech entities,³⁹ the Money Laundering (Prevention and Prohibition) Act 2022 governs virtual asset service providers,⁴⁰ and the Pan-African Payment and Settlement System, launched in 2022, provides settlement infrastructure for AfCFTA-enabled trade.⁴¹ The clearest illustration of the coordination problem this layered structure produces is the continuing contest over digital lending. The FCCPC's 2022 interim framework, since replaced by the 2025 Digital Lending Regulations,⁴²⁴³ requires loan-app registration and consumer-protection compliance, yet section 65(1)(a) of the Banks and Other Financial Institutions Act 2020 excludes CBN-licensed institutions from the FCCPA's reach altogether, leading commentary to characterise the FCCPC's guidelines as a possible usurpation of the Central Bank's exclusive domain.⁴⁴ The Commission has nonetheless

³⁷Central Bank of Nigeria, Regulatory Framework for Open Banking in Nigeria (February 2021) <<https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf>>.

³⁸*ibid*, requiring API Providers and API Consumers to comply with data-sharing, consent and incident-classification obligations under the Guidelines.

³⁹Central Bank of Nigeria, Reviewed Guidelines on International Money Transfer Services in Nigeria (31 January 2024).

⁴⁰Money Laundering (Prevention and Prohibition) Act 2022, discussed in Lexology (n 53) on virtual asset service providers.

⁴¹The Pan-African Payment and Settlement System launched 13 January 2022: AllAfrica (2025).

⁴²Federal Competition and Consumer Protection Commission, Limited Interim Regulatory/Registration Framework and Guidelines for Digital Lending 2022, issued August 2022.

⁴³FCCPC, Digital, Electronic, Online or Non-Traditional Consumer Lending Regulations 2025, gazetted under ss 17, 18 and 163 FCCPA 2018.

⁴⁴Banks and Other Financial Institutions Act 2020, s 65(1)(a); Gelias, 'FCCPC Guidelines on Digital Lending'.

exercised direct enforcement, including orders compelling Google LLC to remove non-compliant lending applications from the Play Store.⁴⁵ Nigeria's digital lending platforms therefore operate under two regulators whose jurisdiction has not been definitively reconciled, a live example of the institutional coordination gap developed further in Part II.C.5 and II.C.6.

6. Institutional Architecture and Enforcement Capacity

The layers above are administered by institutions with different mandates and enforcement tools, and it is this institutional layer, more than the statutory text, that determines whether a cross-border transaction is coherently regulated. The Nigeria Data Protection Commission's powers are limited to personal data processing;⁴⁶ the cybersecurity institutions created by the 2024 Amendment report through the Office of the National Security Adviser and are oriented toward incident response rather than ex ante regulation;⁴⁷ the Federal Competition and Consumer Protection Commission sits within the Ministry of Trade and Investment, oriented toward market conduct;⁴⁸ and the Central Bank regulates payment infrastructure while itself intervening directly in cybersecurity policy, as the 2024 levy episode shows. No statute creates a standing coordination mechanism across these four institutions. Where a single set of facts, such as a cross-border data breach at a foreign-domiciled payment processor, implicates all four regulatory domains at once, each institution has an independent statutory basis to act, but none specifies which leads, how information is shared, or how one regulatory response rather than four

⁴⁵FCCPC, 'Registration of Digital Money Lenders' (2023), recording orders to Google LLC to remove non-compliant lending apps from the Play Store.

⁴⁶AB Legal Practitioners (n 35), referencing the National Cybersecurity Policy and Strategy 2021.

⁴⁷Federal Competition and Consumer Protection Act 2018 (n 42), establishing the Federal Competition and Consumer Protection Commission.

⁴⁸Nigeria Data Protection Act 2023, ss 42(3) and 44 (n 20).

uncoordinated ones is to be produced. The digital lending dispute described in Part II.A.5 is not a hypothetical illustration of this problem; it is the problem, already litigated in substance if not yet in a single unifying judgment.

B. Comparative Frameworks

The four comparator jurisdictions were chosen because each address, in a different way, the specific problem Nigeria's own framework leaves open: how to permit necessary cross-border data flows while retaining an enforceable domestic standard of protection.

1. European Union

The GDPR's Chapter V, articles 44 to 50, is the model the NDPA's own Part VIII most closely follows.⁴⁹ Article 45 allows the European Commission to issue adequacy decisions for a defined, published list of jurisdictions,⁵⁰ and the Court of Justice's Schrems II decision shows adequacy is neither static nor formal, invalidating the EU-US Privacy Shield on the ground that US surveillance law did not in substance match EU protection.⁵¹ The lesson for Nigeria is that an adequacy mechanism requires an active, published, periodically reviewed list to function as more than a paper standard, as Nigeria's own Ikigai litigation already demonstrates domestically.⁵²

2. South Africa

South Africa's Protection of Personal Information Act 4 of 2013 restricts cross-border transfers under section 72, recognising adequacy, consent, contractual necessity, and the data subject's own interest as

⁴⁹AB Legal Practitioners (n 62).

⁵⁰Federal Competition and Consumer Protection Act 2018 (n 63).

⁵¹TechHive Advisory (n 64).

⁵²GDPR (n 1) ch V, arts 44–50.

lawful bases.⁵³ The structural similarity to the NDPA's sections 41 to 43 makes South African commentary instructive: POPIA names no country as affording adequate protection, and the Information Regulator has no formal adequacy-recognition procedure, leaving the burden on the responsible party transfer by transfer.⁵⁴⁵⁵ South Africa is thus a cautionary parallel rather than a model: an adequacy-based statute enacted without administrative infrastructure to make determinations in practice, a risk Nigeria's own Ikigai litigation shows is not merely theoretical.

3. Kenya

Kenya's Data Protection Act 2019 governs cross-border transfers under section 48, requiring the Office of the Data Protection Commissioner to be satisfied that the recipient offers equal or stronger protection.⁵⁶ Kenya adds a feature absent from the NDPA and POPIA: section 50 requires at least one serving copy of personal data to remain on Kenya-based infrastructure regardless of transfer abroad.⁵⁷ The regulator has also pursued cross-border accountability in practice, a 2025 determination against a Ugandan bank formally engaging Uganda's data protection authority, cooperation Nigeria's Commission has not yet been reported to undertake.⁵⁸ For Nigeria, Kenya shows that data-localisation can coexist with an adequacy-based regime, and that cross-border enforcement cooperation between African authorities is achievable now, not merely an AfCFTA-era aspiration.

⁵³GDPR (n 1) art 45.

⁵⁴Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II) [2020] ECLI:EU:C: 2020:559.

⁵⁵Ikigai (n 21).

⁵⁶J Coetzee, 'Cross-Border Data Flows and POPIA (Part II)' (2024) 27 Potchefstroom Electronic Law Journal 48.

⁵⁷ibid, on the absence of a formal adequacy-recognition procedure comparable to the European Commission's.

⁵⁸CMS Law, 'Managing Cross-Border Data Transfers', on POPIA's extension of protection to juristic persons.

4. Singapore

Singapore's Personal Data Protection Act 2012 takes a different approach: section 26 permits transfer where the recipient is bound by enforceable obligations to provide comparable, not identical, protection.⁵⁹ The Personal Data Protection Regulations 2021 operationalise this through contractual safeguards, binding corporate rules, and certification schemes such as the APEC Cross-Border Privacy Rules system.⁶⁰ Singapore has deliberately avoided any data-localisation requirement, reflecting its reliance on cross-border data flows as a structural feature of its financial services economy.⁶¹

5. Comparative Synthesis

Set side by side, the four comparators point toward institutional preconditions rather than a single correct model. The European Union shows that adequacy requires an actively maintained list backed by judicial willingness to test it against substance.⁶² South Africa shows what happens when the same model is enacted without that follow-through: the statutory standard survives, but its content is left to private parties. Kenya shows that data-localisation can be layered onto adequacy without displacing it, and that a regional authority can act cross-border even ahead of continental instruments.⁶³ Singapore shows that comparable, contractually assessed protection is a viable lighter-touch alternative, backed by detailed regulatory guidance.⁶⁴ None of

⁵⁹Recording Law, 'Kenya Data Privacy Laws: DPA 2019, ODPC Enforcement, and 2026 Compliance Guide' (2026).

⁶⁰Manwa Advocates, 'Data Protection Compliance in Kenya for Foreign Companies'.

⁶¹Personal Data Protection Regulations 2021 (Singapore); OECD.AI, PDPA s 26 (2026).

⁶²ResGuard, 'Cross-Border Data Transfers from Singapore: PDPA Requirements and Practical Solutions' (5 February 2026) <<https://resguard-solutions.com/blog/en/singapore-cross-border-data-transfers/>>.

⁶³GDPR (n 1) art 45 (n 71).

⁶⁴Coetzee (n 76, 77).

the four has fully solved the fourth-order problem this article identifies in Part II.C.5, institutional coordination across data protection, cybersecurity and consumer protection regulators, though the European Union's arrangement, coordinating national authorities through the European Data Protection Board, is the most developed attempt on record.⁶⁵ This suggests that Nigeria's reform priority should be to borrow the specific institutional feature each comparator demonstrates works, while treating the coordination problem, and the digital-lending contest described in Part II.A.5, as one it will need to solve largely on its own terms.

C. Identifying the Gaps

Set against this comparative background, and against Nigeria's own judicial and enforcement record, six gaps in the current arrangement stand out. Each is a gap between statutes, institutions or enforcement practices rather than a defect internal to any single one.

1. The Unresolved Content of 'Adequacy' under Sections 41 to 43

The structural allocation between sections 41, 42 and 43 of the NDPA is reasonably clear on the text and the Commission's 2025 Directive.⁶⁶ What is not yet clear, more than three years after commencement, is the substantive content of an adequacy determination: no jurisdiction has been declared adequate, no template contractual clauses have been published, and no guidance comparable to the European Commission's own explains what the Commission will weigh. Nigeria's own Ikigai litigation shows this is not hypothetical: a Nigerian court has already found a predecessor regulator's adequacy list wanting on exactly the grounds Schrems II identifies as the substantive core of adequacy.^{67,68}

⁶⁵Kenya Data Protection Act 2019, ss 48, 50 (n 79, 80).

⁶⁶NDPA 2023, ss 41–43 (n 14–16); GAID 2025 (n 18).

⁶⁷Ikigai (n 21–24).

⁶⁸Schrems II (n 72).

South Africa's structurally similar section 72 confirms that a statute can specify adequacy as the primary transfer basis and still leave it without operative content absent institutional follow-through.⁶⁹

2. Disconnection between the Data-Privacy, Cybersecurity, E-Commerce and Payment Statutes

The NDPA, the Cybercrimes Act as amended, the Electronic Transactions Act and FCCPA, and the Central Bank's payment directives were enacted separately and are administered by four institutions. The only point of express statutory contact is narrow: a data-retention obligation under the 2024 Cybercrimes Amendment that cross-refers to NDPA compliance.⁷⁰ No equivalent link exists between cybersecurity incident-reporting and NDPA breach notification, or between either regime and the Central Bank's Open Banking rules. A single cross-border transaction can therefore trigger obligations under all four regimes without any prescribing how to reconcile compliance across the others, a diagnosis comparative literature on Nigeria's e-commerce framework confirms.⁷¹

3. The AfCFTA Digital Trade Protocol Implementation Gap

Nigeria ratified the AfCFTA's Protocol on Digital Trade in February 2024, establishing a common African framework for electronic transactions, digital payments, consumer protection, data governance and cybersecurity.⁷² Its practical effect remains constrained: eight annexes, including those on Cross-Border Data Transfers and Digital Payments, remain under negotiation.⁷³ Nigeria's own NDPA and

⁶⁹Coetzee (n 76, 77).

⁷⁰AB Legal Practitioners (n 35, 37), on the 2024 Cybercrimes Amendment's cross-reference to NDPA compliance.

⁷¹Nwafor and others (n 47).

⁷²AfCFTA Protocol on Digital Trade, adopted February 2024; IISD (n 4).

⁷³IISD (n 4), on the eight outstanding annexes, including Cross-Border Data Transfers and Cross-Border Digital Payments.

Electronic Transactions Act predate the Protocol and were not drafted with its eventual commitments in view; comparative work has flagged tension between the NDPA's transfer conditions and the Protocol's data-interoperability commitments, risking Nigeria's own law operating as a non-tariff barrier to the trade it has just ratified into.⁷⁴ Kenya's more proactive compliance posture throws Nigeria's slower alignment into relief.⁷⁵

4. Absence of a Cross-Border Consumer-Protection and Dispute-Resolution Channel

None of the three Nigerian statutes gives the FCCPC, the Nigeria Data Protection Commission, or the cybersecurity institutions an international cooperation mechanism comparable to Kenya's willingness to engage a foreign regulator directly, or to the WTO's Joint Statement Initiative on E-Commerce, of which Nigeria is a signatory.⁷⁶ Where a platform is domiciled outside Nigeria, the FCCPA and Electronic Transactions Act offer a domestic right of complaint but no mechanism for the Commission to pursue enforcement against a foreign counterparty, leaving jurisdictional questions largely unresolved in practice.⁷⁷

5. The Institutional Coordination Gap

The absence of a coordination mechanism across the Nigeria Data Protection Commission, the cybersecurity institutions, the FCCPC and the Central Bank, described in Part II.A.6, is distinct from the narrower cross-referencing gap in Part II.C.2 and arguably more consequential. A statute can cross-reference another's standard, as the

⁷⁴Nwafor and others (n 47), on the risk of Nigeria's data protection law acting as a non-tariff barrier to AfCFTA trade.

⁷⁵*ibid*, on Kenya's comparatively more proactive AfCFTA compliance posture.

⁷⁶Manwa Advocates (n 82).

⁷⁷Nwafor and others (n 47), on the FCCPC's lack of a WTO-style dispute mechanism.

2024 Amendment does with the NDPA, without telling the institutions which leads when a single set of facts triggers all four simultaneously.⁷⁸ None of the comparator jurisdictions has solved this comprehensively; even the European Union's coordination through the European Data Protection Board shows the problem persists in a far more mature environment.⁷⁹ Nigeria's arrangement lacks even the basic first step: a statutory obligation to share information and designate a lead regulator. The practical cost falls disproportionately on small and medium-sized enterprises trading under AfCFTA, since these are least able to absorb the compliance cost of navigating uncoordinated regulatory relationships.⁸⁰

6. Payment Infrastructure Divergence and the Digital Lending Precedent

Part II.A.5's account of Central Bank regulation reveals a sixth, more concrete gap: the boundary between the Central Bank's exclusive jurisdiction over licensed institutions and the FCCPC's general consumer-protection mandate has not been settled, and the overlap has already produced a live dispute rather than a theoretical one. Payment Solution and Terminal Service Provider licensees must satisfy Central Bank data-protection conditions,⁸¹ and Open Banking participants separately owe data-sharing obligations to the Central Bank,⁸² neither reconciled with the NDPA's own requirements. Cross-border settlement is further constrained by International Money Transfer Operator rules excluding banks and fintechs from direct

⁷⁸AB Legal Practitioners (n 35, 37, 100).

⁷⁹GDPR (n 95).

⁸⁰Nwafor and others (n 47, 106), on the compliance burden borne by SMEs trading under the AfCFTA framework.

⁸¹Legal 500 (n 49); 618 Bees (n 48).

⁸²Central Bank of Nigeria, Operational Guidelines for Open Banking in Nigeria (n 51, 52).

participation,⁸³ channelling payment volume through intermediaries whose obligations run to the Central Bank rather than uniformly to the Commission. The digital lending dispute is the clearest evidence this divergence is not academic: practitioner analysis has characterised the FCCPC's guidelines as potentially exceeding its authority given that section 65(1)(a) BOFIA 2020 excludes Central Bank-licensed institutions from the FCCPA altogether,⁸⁴ yet the Commission has proceeded to enforce directly, including by directing Google LLC to remove non-compliant applications from the Play Store, without any reported joint enforcement arrangement with the Central Bank. Until this boundary is settled by statute, cross-border payment and lending platforms will continue to face two regulators, each asserting jurisdiction on plausible grounds, with no shared standard between them.

III. SUMMARY OF FINDINGS

This Part draws together the five gaps identified in Part II.C. The NDPA's adequacy mechanism has operative form but no operative content, leaving controllers to self-assess against an unpublished standard. The four regimes cross-reference each other at only one point, the 2024 Cybercrimes Amendment's link to NDPA breach reporting. Nigeria's 2024 AfCFTA ratification has outpaced its domestic legislative programme. No Nigerian consumer has access to a dedicated cross-border dispute-resolution channel, unlike Kenya or Singapore. And the FCCPC-CBN contest over digital lending shows the absence of a lead-regulator rule is a live, unresolved dispute rather than a theoretical risk. Individually, each gap could be read as a drafting omission correctable in isolation. Read together, they describe

⁸³Lex ology (n 53), on restrictions on non-bank International Money Transfer Operator licensing.

⁸⁴Gelias (n 61), analyzing the FCCPC Guidelines as overreach into the CBN's domain under s 65(1)(a) BOFIA 2020.

a single problem: Nigeria's cross-border digital economy is governed by four statutes and one set of central bank directives never designed, or since amended, to operate as a coordinated system.

IV. CONCLUSION

Nigeria has, within a decade, enacted a data protection statute, substantially amended its cybersecurity statute, passed a dedicated electronic transactions statute, and layered payment-system directives atop all three, while ratifying a continental digital trade protocol. Each achievement is real, but they do not yet add up to a coherent regime for cross-border transactions. The NDPA's adequacy mechanism lacks operative content, notwithstanding a judicial precedent already showing Nigerian courts are prepared to test such determinations on their substance.⁸⁵ The four regimes cross-reference each other at only one narrow point.⁸⁶ Domestic law has not caught up with Nigeria's own AfCFTA commitments, and no institution has a cross-border cooperation channel comparable to Kenya's. Most concretely, the FCCPC-CBN contest over digital lending shows institutional coordination is a present, unresolved dispute. These are not drafting failures within any one statute; they are gaps between statutes and institutions that will not close until Nigeria treats cross-border e-commerce, data privacy, cybersecurity and payment regulation as a single regulatory problem.

V. RECOMMENDATION(S)

The gaps identified above share a common feature: none can be closed by amending any single instrument in isolation, because each arises at the boundary between instruments. Four reform priorities follow. First, the Nigeria Data Protection Commission needs a published, periodically reviewed adequacy framework with template transfer

⁸⁵NDPA 2023, ss 41–43 (n 14–17, 90).

⁸⁶AB Legal Practitioners (n 35, 37).

instruments, following the European model and what Nigeria's own *Ikigai* litigation shows courts are prepared to compel.⁸⁷ Second, the 2024 Cybercrimes Amendment's cross-reference to the NDPA needs extending, by statute, to a shared incident-and-breach notification standard spanning the Electronic Transactions Act's disclosure obligations and the Central Bank's data-sharing rules.⁸⁸ Third, Nigeria's legislative programme needs express alignment with its AfCFTA commitments before, not after, the Protocol's outstanding annexes are settled, so Nigeria shapes rather than merely retrofits to that continental negotiation; Kenya's combined adequacy and data-localisation architecture offers the closest regional template.⁸⁹ Fourth, and following from the institutional coordination gap rather than the comparative jurisdictions directly, Nigeria's legislative programme could address this more directly than the European Union's own arrangement has managed, by placing a single statutory obligation on the Nigeria Data Protection Commission, the Computer Emergency Response Teams, the FCCPC and the Central Bank to share information and designate a lead regulator whenever a single set of facts falls within more than one institution's jurisdiction. The digital lending dispute described in Part II.A.5 and II.C.6 is the most urgent candidate for such a reform, since the coordination failure has already produced conflicting regulatory claims rather than remaining a latent risk. This need not require a new super-regulator; it requires only a statutory information-sharing and lead-designation duty of the kind none of the four regimes currently imposes.⁹⁰ The fuller institutional design of a coordinating body across these four institutions is developed elsewhere in this research programme. This article's purpose has been narrower: to establish, through direct comparison

⁸⁷GDPR (n 70, 71).

⁸⁸AB Legal Practitioners (n 35, 37, 100, 114).

⁸⁹Kenya Data Protection Act 2019 (n 79, 80, 92).

⁹⁰IISD (n 4, 103, 105); Diplomatic Times Online (n 104).

with the European Union, South Africa, Kenya and Singapore, and through Nigeria's own judicial and enforcement record, precisely where the current arrangement leaves cross-border digital transactions inadequately governed, so the case for an integrated response rests on demonstrated gaps rather than general assertion.