ARTICLE PAGE

Scan the QR code or use the article URL on this page to open the official article record online.

Global Insights Law Journal
ISSN 3141-5717 | Volume 1 | Issue 3 | Month November | 2026

VOLUME	ISSUE	YEAR
1	3	2026

RESEARCH ARTICLE

A Legal Appraisal of Cybersecurity Challenges in The Resolution of Trade Disputes in Nigeria

Iwunze, Ireju Pamela

PUBLICATION DETAILS
ISSN: 3141-5717 Volume: 1 Issue: 3
Publication Month: November
Publication Year: 2026
DOI URL: https://doi.org/10.67588/0014
Article URL: https://gilawjournal.com/article/a-legal-appraisal-of-cybersecurity-challenges-in-the-resolution-of-trade-disputes-in-nigeria

SCAN ARTICLE

PUBLICATION LICENSES
CC BY 4.0

A LEGAL APPRAISAL OF CYBERSECURITY CHALLENGES IN THE RESOLUTION OF TRADE DISPUTES IN NIGERIA

Iwunze, Ireju Pamela*

Abstract

The rapid digitisation of global commerce, accelerated by electronic contracts, digital trade platforms, cloud computing, and technology-assisted dispute resolution, has fundamentally transformed the landscape of commercial dispute settlement in Nigeria. While digital filing, virtual court proceedings, online dispute resolution (ODR), and electronic arbitration offer unprecedented procedural speed and cost efficiency, they simultaneously expose the administration of commercial justice to unprecedented cybersecurity vulnerabilities. This article undertakes a comprehensive, doctrinal, and comparative legal appraisal of the cybersecurity challenges affecting the resolution of trade disputes in Nigeria. It critically evaluates whether Nigeria's existing legal, regulatory, and procedural framework, principally anchored on the Constitution of the Federal Republic of Nigeria 1999 (as amended), the Cybercrimes (Prohibition, Prevention) Act 2015 (as amended in 2024), the Nigeria Data Protection Act 2023, the Evidence Act 2011 (as amended), and the Arbitration and Mediation Act 2023, adequately safeguards the integrity, confidentiality, availability, authenticity, and final enforceability of trade dispute proceedings. Through a comparative analysis with South Africa and the United Kingdom, the article identifies critical statutory, procedural, and institutional gaps within the Nigerian legal ecosystem, particularly regarding the admissibility of compromised computer-generated evidence, the protection of commercially sensitive trade secrets during virtual hearings, and the cyber liability of legal practitioners, arbitrators, and court administrators. The article concludes that while Nigeria has established foundational cybercrime and data protection legislation, its procedural dispute resolution rules remain dangerously unequipped to address sophisticated cyber threats such as ransomware, Business Email Compromise (BEC), digital identity theft, and deepfake evidence manipulation. To prevent institutional breakdown and preserve commercial trust, the article proposes concrete statutory amendments to the Evidence Act 2011 and Arbitration and Mediation Act 2023, the promulgation of uniform National Judicial Council Practice Directions on Cybersecurity and Virtual Hearings, and the mandatory adoption of institutional cybersecurity protocols across courts and arbitral institutions.

Keywords

Cybersecurity, Trade Dispute Resolution, Electronic Evidence; Cybercrimes Act 2024; Nigeria Data Protection Act 2023; Arbitration and Mediation Act 2023; Online Dispute Resolution; Comparative Commercial Justice.

* Iwunze, Ireju Pamela, LL.B, LB, LLM in view, Rivers State University, irejupiwunze@gmail.com, +2348066002241.

Downloaded from Global Insights Law Journal | gilawjournal.com

1. Introduction

The global economy has entered an era defined by deep technological integration, where international trade, commercial contracting, financial transactions, and supply chain logistics operate almost seamlessly across digital networks. In Nigeria, the expansion of the digital economy, catalysed by the rapid adoption of e-commerce platforms, electronic payment infrastructure, cross-border technology transfers, and the implementation of the African Continental Free Trade Area (AfCFTA) Agreement, has revolutionised commercial interactions. Commercial contracts that were historically negotiated, executed, and archived through physical paper documents are now routinely formed via electronic mail, digital messaging platforms, automated smart contracts, and cloud-based enterprise platforms. Furthermore, financial settlements rely heavily on electronic fund transfers, automated clearinghouse networks, letters of credit processed through digital banking portals, and fintech infrastructure. However, as trade transactions have migrated to digital ecosystems, commercial conflicts and trade disputes have increasingly come to rely on electronic records, digital communications, cloud repositories, and technology-assisted dispute resolution mechanisms.[1]

The deployment of information and communication technology (ICT) in dispute resolution, spanning electronic filing (e-filing) registries, virtual court hearings, digital document repositories, remote witness testimony, online mediation, and fully integrated Online Dispute Resolution (ODR) platforms, offers immense operational advantages. It alleviates severe court congestion, reduces travel expenses, expedites procedural timelines, and enhances access to justice for domestic and international commercial operators. Modern commercial litigation and arbitration are no longer strictly physical proceedings bound by geographic courtrooms; they have evolved into dynamic, data-driven procedural environments where legal arguments, evidence, witness examinations, and tribunal deliberations occur across electronic networks. However this digital transformation introduces a profound legal paradox: the very technology designed to enhance efficiency and access to commercial justice simultaneously exposes the dispute resolution process to complex, sophisticated, and malicious cybersecurity threats.[2]

---

1 Agreement Establishing the African Continental Free Trade Area 2018 (AfCFTA Agreement), art 3*; Olabisi* D Akinkugbe, 'Dispute Settlement under the African Continental Free Trade Area Agreement: A Preliminary Assessment' (2020) 28 *African Journal of International and Comparative Law* 138, 140.

2 Omoniyi Bukola Akinola and Faith Modupe Akinola, 'Court Congestion and Access to Justice in Nigeria: Cancerous or Curable?' (2026) 1(1) *Global Insights Law Journal* 1, 4*; Eirik* Onyema and Monalisa Odibo*, Alternative Dispute Resolution: Multi-Door Courthouses* (British Council 2017) 12.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

Cybersecurity threats in trade dispute resolution manifest across multiple operational vectors. Malicious cyber actors, unscrupulous commercial litigants, hostile foreign state entities, and cybercriminal syndicates increasingly target law firms, arbitral institutions, court registries, expert witnesses, and ODR platforms. Through ransomware attacks that lock digital case files, Business Email Compromise (BEC) schemes that fraudulently divert settlement funds, phishing attacks targeting legal practitioners, unauthorised interception of confidential communications, data breaches exposing commercially sensitive trade secrets, and sophisticated manipulation or deletion of digital evidence, cyber incidents threaten the foundational integrity of the dispute resolution machinery. A successful cyber attack during a trade dispute does not merely inflict financial loss; it compromises the constitutional right to a fair hearing, undermines the authenticity of evidence, breaches commercial confidentiality, interrupts judicial proceedings, and threatens the legal enforceability of resulting court judgements and arbitral awards.[3]

1.1 Statement of the Research Problem

Despite the rapid proliferation of digital dispute resolution tools, legal scholarship and judicial practice in Nigeria have historically treated cybersecurity as an issue external to commercial justice. Existing procedural statutes and court rules treat digital platforms merely as neutral operational conduits, failing to recognise that information security vulnerabilities directly attack the core legal guarantees of commercial adjudication. When a court e-filing registry is hacked, when an unencrypted virtual hearing is intercepted by competitors, or when an electronic contract submitted in evidence is subtly altered by malware, the legal system faces a fundamental breakdown. The central research problem investigated by this article is whether Nigeria's existing legal, procedural, and regulatory framework adequately protects the fairness, confidentiality, evidential integrity, and final enforceability of trade dispute resolution in the face of evolving cybersecurity threats.[4]

3 Constitution of the Federal Republic of Nigeria 1999 (as amended), s 36(1); Bello M Magaji, 'Alternative Dispute Resolution (ADR) as a Mechanism for Managing Industrial Conflicts in Nigeria' (2026) 2(1) *Development Journal of International Affairs, Political Economy and Humanities* 294, 298.

4 Evidence Act 2011 (as amended), s 84; Arbitration and Mediation Act 2023 (AMA 2023), ss 1-15; Lawrence Oyelade Oyeniran, 'An Appraisal of Contemporary Issues in Trade Disputes Resolution in Nigeria' (2024) 6(1) *Kampala International University Law Journal* 1, 8.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

1.2 Principal and Subsidiary Research Questions

This article is organised around the principal research question: 'To what extent does Nigeria's existing legal and institutional framework adequately address cybersecurity challenges affecting the fair, secure, and effective resolution of trade disputes, and what legal and institutional reforms are necessary to strengthen cybersecurity protection within Nigeria's trade dispute resolution system?' To answer this overarching inquiry, the article addresses twelve subsidiary research questions: (1) What is the legal significance of cybersecurity in trade dispute resolution? (2) What forms of trade disputes arise in conventional and digital commerce in Nigeria? (3) What dispute mechanisms are available under Nigerian law? (4) What cybersecurity threats compromise dispute proceedings? (5) How do cyber incidents affect electronic evidence confidentiality, integrity, availability, and admissibility? (6) To what extent do the Cybercrimes Act, Data Protection Act, Evidence Act, and AMA 2023 address cyber risks? (7) What duties and liabilities arise for dispute participants? (8) How should courts and arbitral tribunals handle compromised digital evidence? (9) What procedural safeguards guarantee secure online hearings? (10) How do cyber risks affect cross-border disputes, jurisdiction, and enforcement? (11) What comparative lessons emerge from South Africa and the United Kingdom? (12) What legislative, procedural, and institutional reforms are necessary to secure commercial justice in Nigeria?

1.3 Research Methodology and Analytical Framework

This research adopts a doctrinal legal methodology as its primary research approach, complemented by comparative legal analysis. Doctrinal legal research involves the systematic examination of primary legal authorities, including the 1999 Constitution (as amended), federal statutes, judicial decisions, subsidiary procedural rules, and international treaties, alongside secondary authorities such as academic textbooks, peer-reviewed journal articles, and institutional reports. The comparative analysis evaluates the legal frameworks of South Africa and the United Kingdom, selecting these jurisdictions because they represent mature common law systems that have actively integrated cybersecurity governance into civil procedure, electronic evidence, and commercial arbitration rules.[5]

1.4 Scope and Organisation of the Article

The scope of this article encompasses domestic and international commercial trade disputes resolved in Nigeria via litigation, arbitration, mediation, conciliation, negotiation,

5 C C Wigwe, *Legal Research Methodology and Practice* (Princeton & Associates 2019) 45.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

ODR, and administrative regulatory bodies. The manuscript is organised into sixteen structured sections, progressing logically from conceptual definitions through framework analysis, threat evaluation, evidential examination, statutory review, participant liabilities, comparative study, gap synthesis, reform proposals, and conclusion.[6]

2. Conceptual Foundations of Cybersecurity and Trade Dispute Resolution

A rigorous legal examination of cybersecurity in trade dispute resolution requires establishing precise conceptual clarity. In legal and technical discourse, the terms 'cybersecurity', 'information security', 'data protection', and 'data privacy' are frequently used interchangeably, leading to conceptual confusion and flawed regulatory designs. For the purposes of commercial justice, these concepts must be clearly differentiated while recognising their functional interdependence.[7]

Cybersecurity refers to the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to protect the cyber environment, organisation, and user assets from unauthorised access, attack, damage, or disruption. Information security represents a broader category, encompassing the protection of information assets, whether physical, printed, or digital, from unauthorised access, use, disclosure, disruption, modification, or destruction. Conversely, data protection and data privacy centre specifically on the legal rights of individuals regarding the processing, control, and confidentiality of their personal data, as codified under instruments such as the Nigeria Data Protection Act (NDPA) 2023.[8]

In the specific context of trade dispute resolution, cybersecurity is anchored on six key principles of information security, collectively known as the CIA-AAN triad and resilience framework:

1. Confidentiality: Guaranteeing that commercially sensitive trade secrets, proprietary financial data, strategy documents, and settlement discussions disclosed during dispute proceedings are accessible strictly to authorised participants, legal counsel, arbitrators, or judicial officers.

---

6 ibid, 50.

7 International Telecommunication Union (ITU), *'Definition of Cybersecurity'* (ITU-T Recommendation X.1205, 2008) 2; Nigeria Data Protection Act 2023 (NDPA 2023), s 65.

8 NDPA 2023, ss 24, 39; Cybercrimes (Prohibition, Prevention) Act 2015 (as amended by the Cybercrimes (Prohibition, Prevention) (Amendment) Act 2024), s 58.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

2. Integrity: Ensuring that electronic pleadings, transaction logs, electronic contracts, digital correspondence, and computer-generated evidence presented to a court or arbitral tribunal remain complete, accurate, unaltered, and protected against unauthorised modification or deletion.

3. Availability: Ensuring that digital case management systems, e-filing registries, virtual hearing platforms, and electronic document repositories remain continuously accessible to litigants, counsel, and judges without malicious denial-of-service disruptions or ransomware lockouts.

4. Authenticity: Verifying the true identity of digital communicants, witnesses testifying remotely, signatories to electronic contracts, and the legitimate source of submitted computer-generated records.

5. Non-Repudiation: Providing undeniable technical and legal proof that an electronic transaction, contractual communication, digital filing, or procedural direction originated from a specific party, preventing subsequent fraudulent denial.

6. Cyber Resilience: The operational capacity of dispute resolution institutions, law firms, and platforms to withstand, adapt to, recover from, and maintain procedural continuity during and after a severe cyber incident.

These cybersecurity principles directly intersect with fundamental constitutional and procedural requirements of commercial adjudication. Under Section 36(1) of the Constitution of the Federal Republic of Nigeria 1999 (as amended), every commercial litigant is guaranteed the fundamental right to a fair hearing within a reasonable time by an independent and impartial court or tribunal. When a cybersecurity incident compromises the integrity or availability of case materials, such as when ransomware encrypts an electronic trial bundle or when a Business Email Compromise (BEC) attack alters a submitted contract, the constitutional principle of 'equality of arms' is violated. If one party is deprived of access to evidence or if proceedings are conducted over an insecure platform susceptible to eavesdropping, procedural fairness is irremediably corrupted, rendering resulting decisions vulnerable to setting aside on appeal or refusal of enforcement.[9]

In addition to fair hearing concerns, commercial confidentiality constitutes a core foundation of corporate dispute settlement, particularly in international commercial arbitration

9 *Constitution of the Federal Republic of Nigeria 1999 (as amended), s 36(1); Adene v Dantata* (2003) 4 NWLR (Pt 811) 555 at 570.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

and private mediation. Unlike public litigation, where court records are generally open to public inspection under Section 36(3) of the 1999 Constitution, commercial arbitration offers parties a private, confidential forum where trade secrets, pricing algorithms, proprietary manufacturing processes, and internal corporate valuations remain protected from public exposure and competitor exploitation. When a cyber breach exfiltrates confidential arbitral pleadings, witness statements, or expert valuation reports, the primary commercial incentive for electing arbitration is destroyed. The victimised enterprise suffers immediate market devaluation, competitive injury, and reputational damage, exposing defaulting legal representatives or arbitral institutions to civil claims.[10]

Furthermore, trade disputes in Nigeria span diverse commercial sectors, each presenting distinct cybersecurity vulnerabilities. These include contractual sales disputes, international supply and distribution conflicts, banking and electronic payment settlement disputes, insurance claims, shipping and maritime logistics disputes, construction infrastructure conflicts, intellectual property infringement disputes, and digital marketplace e-commerce claims. Distinguishing trade disputes from pure cybercrime prosecutions is essential: while cybercrime focuses on criminal culpability and state punishment under statutes such as the Cybercrimes Act 2024, trade dispute resolution centres on civil rights, commercial liability, evidential authenticity, and contractual remedies.[11]

For instance, in banking and financial payment disputes, cyber incidents frequently involve unauthorised SWIFT payment interceptions, fraudulent modification of electronic Letters of Credit (LCs), or fintech payment gateway breaches. In maritime shipping and logistics disputes, cyber attacks on digital bills of lading or port tracking databases can alter cargo ownership records, creating complex multi-jurisdictional bailment claims. In digital e-commerce marketplace disputes, platform server breaches can compromise thousands of consumer transactions, raising complex questions regarding platform liability, digital signature verification, and automated dispute resolution integrity.[12]

---

10 *Arbitration and Mediation Act 2023 (AMA 2023), s 62; Chioma Kanu Agomo, Nigerian Employment and Labour Relations Law and Practice (Concept Publications 2011) 295.*

11 Cybercrimes Act 2024, ss 6-14; Evidence Act 2011 (as amended), s 84.

12 Companies and Allied Matters Act 2020 (CAMA 2020), s 868; Federal Competition and Consumer Protection Act 2018 (FCCPA 2018), s 111.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

3. Legal and Institutional Framework for Trade Dispute Resolution in Nigeria

Trade dispute resolution in Nigeria is conducted through a multi-tiered legal and institutional architecture comprising court litigation, statutory arbitration, court-connected and private mediation, commercial conciliation, direct negotiation, and emerging technology-assisted Online Dispute Resolution (ODR) mechanisms. Examining how cybersecurity is regulated across these procedural mechanisms reveals a fragmented, uneven landscape.[13]

In commercial litigation, judicial adjudication is anchored on Section 6 of the 1999 Constitution, which vests judicial powers in Superior Courts of Record. Primary jurisdiction over trade and commercial disputes is divided between the Federal High Court under Section 251 (governing banking, aviation, maritime, customs, intellectual property, and corporate matters under the Companies and Allied Matters Act 2020) and State High Courts under Section 272 (governing general contractual, property, and commercial claims). To modernise court operations, several judicial divisions, notably the High Court of Lagos State, the Federal High Court, and the National Industrial Court of Nigeria (NICN), have introduced electronic filing (e-filing) systems, digital cause lists, and practice directions authorising virtual court hearings via videoconferencing platforms.[14]

However, a critical statutory defect in Nigeria's civil procedure rules is the complete absence of mandatory cybersecurity standards for court technology. Practice directions governing virtual hearings, such as the National Judicial Council (NJC) Guidelines for Virtual Court Proceedings 2020, focus almost exclusively on procedural convenience, bandwidth requirements, and witness visibility, containing no binding technical specifications for end-to-end encryption, multi-factor authentication (MFA), secure cloud storage of trial records, or protocol responses to platform hacking. Consequently, court e-filing registries and virtual courtrooms operate on commercial third-party platforms that lack robust cyber defence architectures, leaving judicial records vulnerable to interception or deletion.[15]

Moreover, court e-filing portals require litigants and law firms to upload electronic pleadings, affidavits, and documentary exhibits over public internet links. In many judicial

13 Sam Erugo, *Introduction to Nigerian Labour Law (*2nd edn, Princeton & Associates 2019) 140.

14 Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 6, 251, 272; Companies and Allied Matters Act 2020 (CAMA 2020), s 868; National Industrial Court of Nigeria Alternative Dispute Resolution (ADR) Centre Rules 2015, O 5.

15 NJC Guidelines for Virtual Court Proceedings 2020; Akinola and Akinola (n 2).

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

divisions, these document repositories are hosted on commercial cloud servers without mandatory cryptographic hash logging or automated vulnerability scans. If an unauthorised intruder accesses a court registry server and replaces a filed commercial agreement with an altered digital copy, court personnel possess no automated technical mechanism to detect the alteration. When the court subsequently proceeds to adjudicate the dispute based on the compromised electronic court file, the judicial process becomes an instrument of injustice.[16]

In alternative dispute resolution, commercial arbitration has undergone significant modernisation following the enactment of the Arbitration and Mediation Act (AMA) 2023, which repealed the obsolete Arbitration and Conciliation Act (ACA) 1988. Section 53 of the AMA 2023 explicitly recognises the validity of electronic arbitration agreements, digital communications, and technology-assisted arbitral hearings. Furthermore, Section 62 of the AMA 2023 establishes a statutory framework for commercial mediation, empowering mediators to utilise remote communication technologies. However, while the AMA 2023 grants arbitrators and mediators broad discretion to determine procedural matters, it contains no explicit statutory mandate requiring tribunals or arbitral institutions to adopt cybersecurity protocols. Unless the parties expressly incorporate institutional rules that specify data security measures, such as the LCIA or ICC Rules, arbitral tribunals possess no explicit statutory guidance regarding cyber risk allocation or evidence protection.[17]

Beyond litigation and arbitration, regulatory and institutional complaint handling mechanisms play a vital role in resolving trade conflicts in specific commercial sectors. Regulatory bodies such as the Federal Competition and Consumer Protection Commission (FCCPC) under the Federal Competition and Consumer Protection Act (FCCPA) 2018, the Central Bank of Nigeria (CBN) Consumer Protection Department, the Nigerian Communications Commission (NCC), the National Information Technology Development Agency (NITDA), and the Nigeria Data Protection Commission (NDPC) superintend administrative dispute resolution frameworks. While these regulators handle thousands of commercial complaints annually, their digital portals frequently process commercially

16 Evidence Act 2011 (as amended), s 84; Lawrence Oyelade Oyeniran, 'An Appraisal of Contemporary Issues in Trade Disputes Resolution in Nigeria' (2024) 6(1) *Kampala International University Law Journal* 1, 14.

17 AMA 2023, ss 53, 62; Celestine Ugonabo and others, 'A Critical Review of Arbitration and Mediation Act 2023' (2026) 12(2) *Tropical Built Environment Journal* 9, 14; Damilola Seun Adesanya, 'A Review of Part II of The Arbitration and Mediation Act 2023' (2023) *BACOLAW Publications* 1, 5.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

sensitive corporate data without transparent cybersecurity audits, creating unquantified cyber risks for corporate complainants.[18]

4. Cybersecurity Threats Affecting Trade Dispute Resolution in Nigeria

To properly assess the legal impact of cybersecurity on trade dispute resolution, it is necessary to examine the specific technical threat vectors that jeopardise proceedings in Nigeria. Cyber threats targeting trade dispute resolution operate across three distinct stages: pre-proceeding evidence gathering, active dispute adjudication, and post-judgement/award enforcement.[19]

A critical legal evaluation reveals eighteen distinct cybersecurity threat vectors that compromise trade dispute resolution:

1. Unauthorised System Access & Hacking: Malicious intrusion into law firm servers, court registries, or arbitral repositories to exfiltrate confidential case strategies, trade secrets, or financial records.

2. Ransomware Attacks: Encrypting electronic trial bundles, judicial databases, or law firm files, demanding ransom payments, and causing total procedural paralysis.

3. Phishing & Social Engineering: Deceptive communications targeting judges, arbitrators, or legal counsel to harvest credentials or deploy malware into dispute networks.

4. Business Email Compromise (BEC): Fraudulent interception of commercial communications, leading parties to deposit settlement funds into fraudulent bank accounts.

5. Digital Identity Theft & Impersonation: Unauthorised actors fraudulently assuming the identity of legal representatives, expert witnesses, or corporate officers during remote virtual hearings.

6. Interception of Confidential Communications: Eavesdropping on unencrypted email exchanges, without-prejudice mediation settlement discussions, or private arbitral tribunal deliberations.

7. Unauthorised Alteration of Digital Evidence: Maliciously modifying electronic contracts, bank transaction logs, audit trails, or digital correspondence submitted as trial exhibits.

---

18 Federal Competition and Consumer Protection Act 2018 (FCCPA 2018), ss 17, 111; NDPA 2023, ss 5, 40; Oyeniran (n 4) 15.

19 International Chamber of Commerce (ICC), *ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration* (2020 edn) 4.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

8. Deletion & Destruction of Electronic Records: Cyber attacks engineered to wipe cloud storage repositories, eliminating critical documentary evidence necessary to establish liability.

9. Distributed Denial-of-Service (DDoS) Attacks: Flooding court e-filing portals or ODR servers with automated traffic, knocking digital dispute platforms offline during limitation deadlines.

10. Compromise of Cloud Repositories: Exploiting weak access controls in third-party cloud storage hosting trial bundles, exposing confidential corporate documents to public leaks.

11. Insecure Video Conferencing Platforms: Conducting virtual hearings over unencrypted or poorly configured platforms, resulting in unauthorised recording, 'Zoom-bombing', or eavesdropping.

12. Malware-Infected Trial Bundles: Embedding trojan viruses or spyware inside submitted PDF electronic trial bundles, compromising the recipient court or law firm network upon opening.

13. Insider Threats: Corrupt or compromised court clerks, IT administrators, or arbitral secretaries abusing legitimate access rights to leak or alter digital records.

14. Compromise of Digital Signatures & Credentials: Forging electronic signatures or hijacking digital certificates used to authenticate settlement agreements or consent orders.

15. Data Breaches Exposing Commercially Sensitive Information: Public exposure of trade secrets, patent specifications, or financial pricing models disclosed under protective confidentiality orders.

16. Unlawful Cross-Border Data Access: Foreign state surveillance or extraterritorial cloud subpoenas accessing Nigerian commercial evidence stored on overseas servers.

17. Cyber Attacks on Trade Finance & Payment Systems: Hacking electronic Letters of Credit (LCs) or SWIFT payment networks, creating fraudulent transaction records that trigger commercial disputes.

18. Artificial Intelligence & Deepfake Manipulation: Deploying generative AI to create synthetic audio, deepfake video testimony, or forged electronic signatures presented as authentic trial evidence.

The legal consequences of these cyber threats are devastating to the administration of commercial justice. When ransomware encrypts an arbitral file or when BEC redirects settlement funds, the legal system faces a fundamental crisis. If a court or tribunal unwittingly

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

relies on altered digital evidence, it renders an unconstitutional decision that violates Section 36(1) of the 1999 Constitution. Furthermore, where commercially sensitive trade secrets are leaked due to insecure virtual hearing platforms, the victimised commercial party suffers irreversible market injury, destroying the primary commercial rationale for choosing confidential dispute resolution.[20]

Moreover, in active litigation and arbitration, cyber threat vectors can be weaponised strategically by recalcitrant commercial litigants to obstruct justice. A party facing imminent adverse judgement may launch a covert DDoS attack against an e-filing portal on the final day of a statutory limitation period, deliberately causing time to run out and subsequently raising a limitation defence under statute. Alternatively, a dishonest litigant may engineer a fake ransomware infection on corporate servers to claim an inability to comply with pre-trial document discovery orders. Without a deep understanding of digital forensics and cyber risk management, courts may be vulnerable to procedural manipulation, which could erode public trust in commercial dispute resolution.[21]

5. Cybersecurity, Electronic Evidence and the Administration of Commercial Justice

In modern trade dispute resolution, documentary evidence is overwhelmingly electronic. Commercial contracts, purchase orders, invoices, bank transfer receipts, bills of lading, and corporate correspondence exist predominantly as computer-generated records, emails, text messages, and database entries. Consequently, the legal relationship between cybersecurity and the admissibility, authenticity, and weight of electronic evidence represents one of the most critical battlegrounds in commercial litigation and arbitration.[22]

5.1 The Statutory Mandate of Section 84 of the Evidence Act 2011

Under Nigerian law, the statutory threshold governing the admissibility of computer-generated evidence is codified under Section 84 of the Evidence Act 2011 (as amended). Section 84(1) establishes that in any proceeding where a statement contained in a document

20 Constitution of the Federal Republic of Nigeria 1999 (as amended), s 36(1)*; Western Steel Works Ltd v Iron and Steel Workers Union of Nigeria* (1987) 1 NWLR (Pt 49) 284 at 298.

21 Limitation Law Cap L85 Laws of Lagos State 2015, s 8; Evidence Act 2011 (as amended), s 167(d).

22 Evidence Act 2011 (as amended), s 84; *Kubor v Dickson* (2013) 4 NWLR (Pt 1345) 534 at 550.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

produced by a computer is sought to be given in evidence, the document is admissible, provided the conditions specified under Section 84(2) are satisfied. Section 84(2) requires proof that:

1. The computer-generated document was produced during a period over which the computer was used regularly to store or process information for the purposes of activities regularly carried on.

2. During that period, information of the kind contained in the statement was regularly supplied to the computer.

3. Throughout the material part of that period, the computer was operating properly, or, if not, any respect in which it was not operating properly was not such as to affect the production of the document.

4. The information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of activities.

Furthermore, Section 84(4) mandates the submission of a Certificate of Authentication signed by a responsible officer attesting to the proper operation of the computer system. In a series of landmark judicial decisions, notably *Kubor v Dickson, Dickson v Sylva,* and *Omisore v Aregbesola*, the Supreme Court of Nigeria strictly affirmed that compliance with Section 84 is a non-negotiable statutory condition precedent to the admissibility of computer-generated records.[23]

5.2 Evidential Vulnerabilities in Modern Cyber Incidents

However, a critical legal appraisal of Section 84 reveals profound limitations when confronted with sophisticated cybersecurity incidents. Section 84 was originally designed for traditional, localised computer systems. It fails to adequately address modern cyber threats such as cloud-based data storage, distributed ledger networks, metadata alteration, or AI-generated deepfakes. Under Section 84, a Certificate of Authentication is typically signed by a corporate employee or IT staff member who states that the company computer was operating properly. Crucially, a computer system may appear to be operating 'properly' to a lay employee while simultaneously being infected with covert malware or compromised by an unauthorised intruder who has altered underlying transaction records.[24]

---

23 *Kubor v Dickson* (n 19) 555*; Dickson v Sylva* (2017) 8 NWLR (Pt 1567) 167 at 182*; Omisore v Aregbesola* (2015) 15 NWLR (Pt 1482) 205 at 230.

24 Evidence Act 2011 (as amended), s 84(2)(c); Akinola and Akinola (n 2) 12; Oyeniran (n 4) 18.

License(s): CC BY 4.0
See license terms at creativecommons.org Downloaded from Global Insights Law Journal | gilawjournal.com

5.3 Distinguishing Admissibility, Authenticity, Probative Weight, and Legality of Acquisition

In legal theory, a fundamental distinction must be drawn between admissibility, authenticity, evidential weight, and legality of acquisition. While Section 84 regulates statutory admissibility, a cyber incident directly attacks the authenticity and probative weight of digital evidence. Where a commercial party alleges that an opponent's electronic invoice, bank log, or email trail has been modified via a cyber attack, the court or arbitral tribunal must look beyond formal Section 84 certificates. Proving digital authenticity requires sophisticated digital forensic evidence, including cryptographic hash value verification (such as SHA-256 algorithms), audit log analysis, metadata inspection, and chain of custody preservation under Section 68 of the Evidence Act 2011 governing expert opinion.[25]

5.4 Judicial Remedies, Digital Preservation Orders, and Adverse Inferences

Where digital evidence is compromised or rendered inaccessible due to a ransomware attack or cloud deletion, Nigerian courts and arbitral tribunals must exercise statutory powers to issue preservation orders, Anton Piller inspection orders, or order independent digital forensic audits. Where a party wilfully fails to safeguard digital evidence after receiving notice of a dispute, or where evidence is manipulated, courts must draw adverse inferences under Section 167(d) of the Evidence Act 2011, holding that the unproduced or altered record would have been unfavourable to the spoliator.[26]

Furthermore, in complex commercial litigation, courts must establish clear standards for evaluating generative AI deepfakes. As generative artificial intelligence tools become accessible, fraudulent litigants can synthesise realistic audio recordings or video testimonies of corporate executives agreeing to contractual variations. Verifying AI-generated deepfakes requires forensic audio-visual spectral analysis and source file metadata verification. Judges and arbitrators who lack technical training risk admitting sophisticated synthetic evidence, corrupting the judicial finding of fact and violating the constitutional guarantee of a fair hearing.[27]

---

25 Evidence Act 2011 (as amended), s 68; *Suberu v African Petroleum Plc* (2002) 7 NWLR (Pt 766) 244 at 256.

26 Evidence Act 2011 (as amended), s 167(d); *Federal Government of Nigeria v Academic Staff Union of Universities (ASUU)* (Unreported) Suit No NICN/ABJ/270/2022, ruling delivered 21 September 2022.

27 Evidence Act 2011 (as amended), s 68; *Dickson v Sylva* (n 21) 175; Oyeniran (n 4) 20.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

6. The Cybercrimes Act and the Legal Consequences of Cybersecurity Incidents in Trade Disputes

The substantive statutory framework criminalising cyber threats in Nigeria is codified under the Cybercrimes (Prohibition, Prevention) Act 2015, as amended by the Cybercrimes (Prohibition, Prevention) (Amendment) Act 2024. While the Cybercrimes Act is primarily a penal statute, its provisions directly impact civil trade dispute resolution when cyber incidents occur during commercial transactions or ongoing dispute proceedings.[28]

Key provisions of the Cybercrimes Act 2024 relevant to trade dispute resolution include:

Section 6 (Unauthorised Access to Critical National Information Infrastructure): Criminalising unauthorised access to designated computer systems, which applies directly to hacking attacks targeting court registries, judicial databases, or financial clearinghouses.

Section 7 (System Interference): Penalising the intentional hindrance or disruption of computer systems, providing criminal sanctions against DDoS attacks that knock virtual court platforms offline.

Section 8 (Data Interference): Prohibiting the unauthorised deletion, deterioration, alteration, or suppression of computer data, directly addressing digital evidence tampering in commercial litigation.

Section 13 (Computer-Related Fraud): Criminalising input, alteration, or deletion of computer data to secure fraudulent economic advantage, covering Business Email Compromise (BEC) and forged trade finance records.

Section 14 (Computer-Related Forgery): Penalising the creation of false digital records intended to be acted upon as authentic, covering fake electronic contracts and forged digital signatures.

Section 22 (Identity Theft and Impersonation): Criminalising digital impersonation, covering fraudulent witness impersonation during virtual court hearings.

Section 38 (Duties of Service Providers): Mandating internet service providers to retain traffic data and subscriber information for at least two years, facilitating digital forensic tracing in trade disputes.

Crucially, a sharp legal distinction must be drawn between criminal liability under the Cybercrimes Act and the civil procedural consequences of a cyber incident in a trade dispute.

28 Cybercrimes Act 2024, Preamble, ss 1-3.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

Criminal prosecution under the Cybercrimes Act is initiated by the state to punish offenders, requiring proof beyond a reasonable doubt under Section 135 of the Evidence Act 2011. In contrast, a trade dispute focuses on civil remedies, contractual damages, evidential admissibility, and procedural fairness between private commercial parties, where liability is determined on the balance of probabilities under Section 134 of the Evidence Act 2011. Where a cybercrime investigation occurs concurrently with civil commercial litigation or arbitration, complex legal conflicts arise regarding the impounding of digital evidence, law enforcement access to confidential corporate files under Section 45, and applications to stay civil proceedings pending criminal prosecution.[29]

7. Data Protection, Privacy and Commercial Confidentiality in Trade Dispute Resolution

The processing of information during trade dispute resolution inherently involves handling personal data and commercially sensitive trade secrets. Electronic filings, witness statements, employment files, corporate audit reports, and financial statements contain vast quantities of personal data regulated under the Nigeria Data Protection Act (NDPA) 2023.[30]

Under Section 24 of the NDPA 2023, data controllers and processors, which legally encompass law firms, corporate litigants, arbitral institutions, mediation centres, and court administrators, must process personal data lawfully, fairly, and transparently. Section 25 of the NDPA 2023 provides the legal basis for processing personal data in dispute resolution, specifically where processing is necessary for compliance with a legal obligation or for the establishment, exercise, or defence of legal claims. However, Section 39 of the NDPA 2023 imposes a strict statutory duty on data controllers to implement appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data.[31]

Where a data breach occurs during a trade dispute, such as when an e-filing system is hacked or an unencrypted trial bundle is leaked, Section 40 of the NDPA 2023 mandates that the data controller must notify the Nigeria Data Protection Commission (NDPC) within 72 hours of becoming aware of the breach and inform affected data subjects where the breach poses a high risk to their rights. Furthermore, in cross-border trade arbitration, transferring

29 Cybercrimes Act 2024, ss 38, 45; Evidence Act 2011 (as amended), ss 134, 135; Erugo (n 11) 160.

30 NDPA 2023, ss 1, 24, 39.

31 NDPA 2023, ss 24, 25, 39; Folabi Kuti, 'A Review of 2025 Significant Decisions in Labour and Employment Matters' (2025) National Industrial Court of Nigeria Judgment Portal 1, 14.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

electronic case files across national borders triggers Sections 41 to 43 of the NDPA 2023, requiring proof of adequate data protection mechanisms or explicit statutory derogations for legal proceedings.[32]

A vital legal distinction must be maintained between data protection (which safeguards personal data) and commercial confidentiality (which protects proprietary corporate secrets, financial pricing models, and technical patents). In commercial arbitration and mediation, confidentiality is a primary contractual attraction. When a cybersecurity breach exposes arbitral submissions or mediation disclosures, it breaches contractual confidentiality clauses under Section 62 of the AMA 2023, exposing the defaulting party or institution to civil damages for breach of confidence and loss of commercial advantage.[33]

8. Cybersecurity Duties and Liability of Participants in Trade Dispute Resolution

Establishing a cyber-resilient dispute resolution ecosystem requires defining the specific legal duties and potential civil liabilities of all participants in the dispute processing pipeline:

A. Commercial Parties: Corporate litigants owe contractual duties under commercial agreements to maintain secure communication channels, preserve digital records, and implement cybersecurity safeguards. Unreasonable failure to secure commercial data, leading to evidence destruction, exposes parties to adverse evidential inferences or civil claims for spoliation.

B. Legal Practitioners and Law Firms: Under Rule 14 and Rule 19 of the Rules of Professional Conduct for Legal Practitioners (RPC), lawyers owe strict professional duties of competence, diligence, and client confidentiality. Storing unencrypted client case files on public cloud networks or transmitting unencrypted trial bundles via public email constitutes professional negligence, exposing legal practitioners to disciplinary sanctions and civil malpractice suits.

C. Arbitrators and Arbitral Institutions: Arbitrators owe statutory duties under Section 43 of the AMA 2023 to treat parties with equality and conduct proceedings without delay. Operating over unencrypted video platforms or failing to issue cybersecurity procedural directions

32 NDPA 2023, ss 40, 41-43; Kuti (n 29) 16.

33 AMA 2023, s 62*; Mix and Bake Flour Mill Ltd v National Union of Food, Beverage and Tobacco Employees* (2012) 26 NLLR (Pt 73) 72 at 85*;* Agomo (n 10) 295.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

breaches the arbitral mandate, potentially rendering arbitral awards vulnerable to setting aside under Section 55 of the AMA 2023 for misconduct or procedural irregularity.

D. Mediators and Mediation Providers: Mediators owe strict statutory duties of confidentiality under Section 74 of the AMA 2023. Unsecured transmission of a without-prejudice settlement offers compromises, mediates neutrality and triggers civil liability for breach of statutory duty.

E. Courts and Judicial Administrators: Judicial registries and court IT administrators owe a public law duty under Section 6 of the 1999 Constitution to safeguard the integrity of court files and judicial records. Negligent court registry security resulting in document loss breaches public trust and infringes constitutional access to justice.

F. Technology and Cloud Service Providers: Third-party cloud vendors hosting e-filing registries or virtual courtrooms owe contractual duties under Service Level Agreements (SLAs) and statutory duties as data processors under Section 24 of the NDPA 2023, exposing them to civil damages for platform failure or unauthorised data disclosures.

G. Digital Forensic Experts: Forensic experts evaluating digital evidence owe strict duties of independence, professional competence, and chain of custody preservation under Section 68 of the Evidence Act 2011, exposing them to civil liability for flawed forensic methodology.

9. Cybersecurity, Online Hearings and Procedural Fairness

The widespread adoption of virtual court hearings and remote arbitral sessions has fundamentally reshaped procedural law in Nigeria. However, conducting dispute proceedings over video conferencing platforms introduces complex constitutional questions regarding procedural fairness, open justice, and witness integrity under Section 36 of the 1999 Constitution.[34]

Section 36(3) of the 1999 Constitution mandates that court proceedings shall be held in public. When virtual hearings are conducted over private, password-restricted video links that exclude the general public and press without statutory authorisation, or conversely, when public virtual hearing links are subjected to malicious disruption, known as 'Zoom-bombing' or 'unauthorised public broadcasting', constitutional tensions emerge. Furthermore, in remote witness examination, cybersecurity vulnerabilities create risks of covert witness prompting via

34 Constitution of the Federal Republic of Nigeria 1999 (as amended), s 36(1), (3); *Sahara Energy Resources Limited v Oyebola* (2020) LPELR-51803(CA) 22.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

hidden messaging apps, digital identity impersonation, or AI-enabled deepfake video feeds, directly compromising the court's ability to assess witness demeanour and credibility.[35]

Where a severe cyber incident interrupts a virtual hearing, such as when a DDoS attack disconnects counsel during cross-examination or when platform hacking compromises arbitral deliberations, the tribunal must grant procedural remedies. These include immediate procedural adjournments, platform migration to encrypted networks, mandatory multi-factor authentication (MFA), protective confidentiality directions, or ordering in-person hearings to preserve procedural integrity. Additionally, judicial authorities must address technological exclusion barriers, ensuring that commercial parties with limited digital capacity are not denied access to justice.[36]

10. Cybersecurity Challenges in Cross-Border Trade Dispute Resolution

Cross-border trade disputes involving Nigerian entities, international commercial counterparties, multi-jurisdictional supply contracts, and transnational digital commerce exacerbate cybersecurity complexity. When a cyber incident occurs during an international arbitration or cross-border commercial litigation, choice of law, extra-territorial jurisdiction, and enforcement questions immediately arise.[37]

In international commercial arbitration governed by the UNCITRAL Model Law and the Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958 (New York Convention), codified under Part III of Nigeria's AMA 2023, a cybersecurity breach during proceedings may jeopardise award enforcement. Under Article V(1)(b) of the New York Convention and Section 55(2)(a)(ii) of the AMA 2023, recognition and enforcement of an arbitral award may be refused if the party against whom the award is invoked was unable to present their case. If a cyber attack deprives a foreign party of access to trial evidence or

35 Constitution of the Federal Republic of Nigeria 1999 (as amended), s 36(3); *Emma Elegbe & Anor v HP International Schools Limited & 3 Ors* (2026) Supreme Court Decision SC/CV/123/2024; Simmons Cooper Partners, 'Employment and Defamation: Supreme Court Clarifies the Proper Forum for Workplace-Related Claims' (2026) *SCP Legal Digest* 1, 3.

36 Emma Elegbe (n 34) 5; Akinola and Akinola (n 2).

37 UNCITRAL Model Law on International Commercial Arbitration 1985 (with 2006 amendments), arts 1, 19; New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958, art V.

License(s): CC BY 4.0
See license terms at creativecommons.org Downloaded from Global Insights Law Journal | gilawjournal.com

compromises arbitral communications, the resulting award faces refusal of enforcement in foreign jurisdictions.[38]

Furthermore, international trade disputes intersect with major global cybersecurity and data protection instruments: the UNCITRAL Model Law on Electronic Commerce (1996), the UNCITRAL Model Law on Electronic Signatures (2001), the UNCITRAL Model Law on Electronic Communications in International Contracts (2005), the Singapore Convention on Mediation (2018), the Council of Europe Budapest Convention on Cybercrime (2001), and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention 2014). While Nigeria signed the Malabo Convention, formal domestication under Section 12 of the 1999 Constitution remains incomplete, creating legislative gaps in cross-border cybercrime cooperation.[39]

11. Comparative Analysis of Cybersecurity and Trade Dispute Resolution in South Africa and the United Kingdom

To identify actionable reform models for Nigeria, a comparative analysis of the legal and institutional frameworks of South Africa and the United Kingdom is essential. These jurisdictions offer mature common law models that have systematically integrated cybersecurity governance into commercial dispute resolution.

11.1 The South African Framework

South Africa represents a leading African comparative model, having established a robust legal architecture comprising the Constitution of the Republic of South Africa 1996, the Cybercrimes Act 19 of 2020, the Protection of Personal Information Act 4 of 2013 (POPIA), the Electronic Communications and Transactions Act 25 of 2002 (ECTA), and the International Arbitration Act 15 of 2017. Under POPIA, South Africa established an independent statutory information regulator clothed with broad enforcement powers over data breaches in judicial and arbitral proceedings. Furthermore, South African courts operate under clear directives on electronic case management and virtual hearings, enforcing strict security standards for digital evidence authentication and cloud storage under ECTA.[40]

---

38 AMA 2023, s 55(2)(a)(ii); New York Convention 1958, art V(1)(b); *P&ID v Nigeria* (2023) High Court of Justice (Commercial Court) CL-2019-000758*, paras 120-135.*

39 Constitution of the Federal Republic of Nigeria 1999 (as amended), s 12; AU Malabo Convention 2014, arts 8-14; Singapore Convention on Mediation 2018, art 3.

40 Protection of Personal Information Act 4 of 2013 (POPIA) (South Africa), ss 39-45; Electronic Communications and Transactions Act 25 of 2002 (ECTA) (South Africa), s 15; Sidumo *v Rustenburg Platinum*

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

Under Section 15 of South Africa's ECTA 2002, the rules of evidence in court and arbitral proceedings expressly accommodate data messages, specifying that the evidential weight of an electronic record is assessed by considering the reliability of the manner in which the record was generated, stored, or communicated, the reliability of the manner in which the integrity of the information was maintained, and the manner in which its originator was identified. This flexible, reliability-focused approach contrasts sharply with Nigeria's rigid Section 84 certificate requirement under the Evidence Act 2011, providing South African courts with greater statutory flexibility to evaluate cyber-compromised digital evidence.[41]

11.2 The United Kingdom Framework

The United Kingdom provides an advanced Commonwealth comparative model, anchored on the Computer Misuse Act 1990, the Data Protection Act 2018 (incorporating the UK GDPR), the Network and Information Systems (NIS) Regulations 2018, the Arbitration Act 1996 (as modernised by the Arbitration Act 2025), and the Civil Procedure Rules (CPR). Section 7 of the UK Arbitration Act 2025 explicitly equips arbitral tribunals with statutory powers to issue summary disposal awards on claims or defences possessing no real prospect of success, preventing recalcitrant parties from deploying fraudulent or cyber-compromised claims. Furthermore, UK courts enforce CPR Practice Direction 31B governing e-disclosure and digital evidence metadata, supported by institutional guidance from the National Cyber Security Centre (NCSC) and the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration.[42]

Under CPR Practice Direction 31B, UK courts mandate that commercial litigants complete an Electronic Documents Questionnaire prior to trial, detailing the hardware, cloud repositories, software, and encryption tools used to preserve electronic documents. Furthermore, Practice Direction 31B regulates the exchange of metadata, hash values, and native file formats, ensuring that questions regarding digital tampering or unauthorised access

---

Mines Ltd (2007) 12 BLLR 1097 (CC) 1108*;* D O Ololube, 'Conflict Management Mechanisms in the Public Sector: A Comparative Study of Nigeria and South Africa' (2025) 7(3) *International Journal of Institutional Leadership, Policy and Management 635,* 638.

41 ECTA 2002 (South Africa), s 15; POPIA 2013, s 22; Geo Quinot, 'Does PAJA Still Form Part of the Legislative Puzzle?' (2020) *De Rebus* 22, 26.

42 UK Arbitration Act 2025, s 7; UK Civil Procedure Rules (CPR), PD 31B; UK Data Protection Act 2018, Sch 1; England Cemented as Key Destination for Arbitration (2025) Pinsent Masons Legal Report 1, 4; The UK Arbitration Act 2025: Key Changes and Summary Disposal (2025) Financier Worldwide 1, 5.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

are resolved transparently before trial. This structured e-disclosure framework provides a powerful procedural model for modernising Nigerian civil procedure.[43]

11.3 Comparative Evaluation

Comparing Nigeria, South Africa, and the United Kingdom across key legal dimensions highlights fundamental structural differences:

1. Statutory Cybercrime Framework: Nigeria (Cybercrimes Act 2024), South Africa (Cybercrimes Act 2020), and the UK (Computer Misuse Act 1990) all possess penal statutes. However, South Africa and the UK integrate cybercrime reporting directly with civil procedure rules.

2. Data Protection and Breach Notification: South Africa (POPIA) and the UK (UK GDPR) mandate strict 72-hour breach notifications overseen by independent regulators, specifically the Information Regulator and Information Commissioner's Office. Nigeria's NDPA 2023 establishes the NDPC, but enforcement within judicial registries remains nascent.

3. Electronic Evidence Authenticity: UK CPR PD 31B and South Africa ECTA Section 15 provides flexible, metadata-driven rules for digital evidence. Nigeria's Section 84 Evidence Act 2011 remains rigid, relying on formal employee certificates that fail against hidden malware.

4. Virtual Hearing Security Rules: The UK and South Africa enforce binding judicial guidelines for virtual hearing security and platform encryption. Nigeria relies on non-binding NJC directions lacking technical security standards.

5. Arbitral Summary Disposal Powers: Section 7 of the UK Arbitration Act 2025 empowers tribunals to summarily dismiss cyber-compromised or fraudulent claims. Nigeria's AMA 2023 contains no explicit summary disposal power.

12. Comparative Lessons for Nigeria

From this comparative analysis, five critical, adaptable legal lessons emerge for modernising Nigeria's trade dispute framework:

1. Adoption of Institutional Cybersecurity Protocols: Nigeria should adopt mandatory cybersecurity protocols modelled after the ICCA-NYC Bar-CPR Protocol, requiring courts and arbitral tribunals to issue cyber risk directions at procedural conferences.

---

43 UK CPR, PD 31B, paras 10-15; UK Data Protection Act 2018, s 11; Reforming Section 67: A New Era for Jurisdictional Challenges (2025) *Dispute Resolution Journal* 1, 4.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

2. Statutory Authorisation for Arbitral Summary Disposal: Amending the AMA 2023 to incorporate summary disposal powers modelled after Section 7 of the UK Arbitration Act 2025, enabling tribunals to summarily dismiss claims built on fraudulent or altered digital evidence.

3. Reform of Electronic Evidence Rules: Amending Section 84 of the Evidence Act 2011 to replace rigid employee certificates with flexible cryptographic hash value verification (SHA-256) and metadata inspection rules modelled after UK CPR PD 31B.

4. Integration of Data Protection Breach Protocols: Establishing direct administrative linkages between the NDPC, court registries, and arbitral institutions to mandate 72-hour breach reporting for leaked legal files, drawing from South Africa POPIA.

5. Mandatory Technical Baseline Standards for Virtual Hearings: Promulgating binding NJC Practice Directions specifying minimum encryption, multi-factor authentication, and secure cloud storage standards for all virtual court proceedings.

13. Challenges and Gaps in Nigeria's Legal and Institutional Framework

Synthesising the analysis reveals six major categories of legal, procedural, and institutional gaps in Nigeria:

1. Statutory Gaps: Absence of explicit cybersecurity mandates in the Evidence Act 2011, AMA 2023, and High Court Civil Procedure Rules.

2. Procedural Gaps: Lack of standardised practice directions regulating virtual hearing security, e-discovery metadata, and platform encryption.

3. Institutional Gaps: Severe technical infrastructure deficits, unencrypted registry servers, and lack of cyber incident response teams in Nigerian courts.

4. Evidential Gaps: Inadequacy of Section 84 Evidence Act 2011 regarding cloud evidence, deepfakes, and automated malware tampering.

5. Regulatory Gaps: Fragmented coordination between NDPC, NITDA, cybercrime law enforcement agencies, and the judicial arm of government.

6. Professional Capacity Gaps: Low cybersecurity awareness, technical literacy deficits, and lack of specialised digital forensic training among legal practitioners, arbitrators, and judges.

14. Legal, Procedural and Institutional Reform Proposals

To construct a secure, cyber-resilient system for resolving trade disputes in Nigeria, the following concrete, draft-ready reform proposals are recommended:

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

1. Statutory Legislative Amendments: a) Amend Section 84 of the Evidence Act 2011 to incorporate statutory provisions for cryptographic hash verification, metadata inspection, and cloud evidence admissibility. b) Amend the AMA 2023 to mandate cybersecurity risk assessments for tribunals and grant explicit summary disposal powers. c) Complete formal legislative domestication of the AU Malabo Convention 2014 under Section 12 of the 1999 Constitution.

2. Promulgation of Judicial Practice Directions: The National Judicial Council (NJC) should issue uniform Practice Directions on Cybersecurity and Virtual Hearings, mandating end-to-end encryption, multi-factor authentication (MFA), secure cloud storage, and protocols for managing virtual hearing disruptions.

3. Institutional Rules Modernisation: Commercial arbitral institutions, such as the Lagos Court of Arbitration (LCA) and the NICN ADR Centre, should amend their institutional rules to incorporate mandatory cybersecurity protocols, data breach notification rules, and cyber risk allocation guidelines.

4. Technical Infrastructure and Baseline Standards: Establish minimum technical baseline standards for court e-filing portals, enforcing SHA-256 cryptographic hash logging for all filed electronic documents, encrypted cloud storage, and annual penetration testing.

5. Capacity Building and Professional Training: The National Judicial Institute (NJI) and the Nigerian Bar Association's Mandatory Continuing Legal Education (NBA-MCLE) framework should establish mandatory cyber-forensics and legal technology training modules for judges, arbitrators, and legal practitioners.

15. Conclusion

This dissertation has conducted a rigorous legal appraisal of the cybersecurity challenges confronting trade dispute resolution in Nigeria. Answering the principal research question, the study demonstrates that Nigeria's existing legal and institutional framework is dangerously incomplete and unequipped to protect the fair, secure, and effective resolution of trade disputes against modern cybersecurity threats. While Nigeria has enacted foundational legislation in cybercrimes (Cybercrimes Act 2024), data protection (NDPA 2023), and arbitration (AMA 2023), these statutory regimes operate in isolation from procedural court rules and evidential standards.

Cybersecurity is not merely a technical IT issue external to commercial justice; it is a fundamental constitutional requirement that directly impacts the fair hearing guarantees under

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

Section 36(1) of the 1999 Constitution, the authenticity of trial evidence, the protection of commercial trade secrets, and the final enforceability of court judgements and arbitral awards. By adopting the comparative lessons of South Africa and the United Kingdom, implementing statutory amendments to the Evidence Act 2011 and AMA 2023, and promulgating uniform NJC Practice Directions on Cybersecurity, Nigeria can construct a modern, cyber-resilient commercial justice framework capable of fostering commercial trust, protecting domestic trade, and advancing continental trade integration under the AfCFTA.

References

Books

Agomo C K, *Nigerian Employment and Labour Relations Law and Practice* (Lagos: Concept Publications 2011).

Aturu B, *Nigerian Labour Laws: Principles, Cases, Commentaries and Materials* (Lagos: Friedrich Ebert Stiftung 2008).

Bingham T*, The Rule of Law* (London: Allen Lane 2010).

Dicey A V, *An Introduction to the Study of the Law of the Constitution* (10th edn, London: Macmillan 1959).

Emiola A, *Nigerian Labour Law* (4th edn, Ogbomoso: Emiola Publishers 2008).

Erugo S, *Introduction to Nigerian Labour Law: Contract of Employment and Labour Practice* (2nd edn, Lagos: Princeton & Associates Publishing Co Ltd, 2019).

Garner, B. A. (ed), *Black's Law Dictionary* (8th edn, St Paul, Minn: West Publishing Co 2004).

Onyema E and Odibo M, *Alternative Dispute Resolution: Multi-Door Courthouses* (London: British Council 2017).

Orojo J O and Ajomo M A, *Law and Practice of Arbitration and Conciliation in Nigeria* (Lagos: Mbeyi & Associates 1999).

Raz J, *The Authority of Law: Essays on Law and Morality* (Oxford: Clarendon Press 1979).

Wade H W R and Forsyth C F*, Administrative Law* (11th edn, Oxford: Oxford University Press 2014).

Journal Articles

Adeogun A A, 'Towards a Better System for Settling Trade Disputes in Nigeria' (1978) 10 *Nigerian Law Journal* 6-25.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

Adesanya D S, 'A Review of Part II of The Arbitration and Mediation Act 2023' (2023) BACOLAW Publications 1-12.

Akinkugbe O D, 'Dispute Settlement under the African Continental Free Trade Area Agreement: A Preliminary Assessment' (2020) 28 *African Journal of International and Comparative Law* 138-158.

Akinola O B and Akinola F M, 'Court Congestion and Access to Justice in Nigeria: Cancerous or Curable?' (2026) 1(1) *Global Insights Law Journal* 1-18.

Magaji B M, 'Alternative Dispute Resolution (ADR) as a Mechanism for Managing Industrial Conflicts in Nigeria' (2026) 2(1*) Development Journal of International Affairs, Political Economy and Humanities* 294-310.

Mamudu J A, 'Trade Dispute Resolution in Nigeria: Mechanisms, Challenges, and Prospects' (2025) 3(1) *International Journal of Advanced Multidisciplinary Academic Research and Development* 26-38.

Ololube D O, 'Conflict Management Mechanisms in the Public Sector: A Comparative Study of Nigeria and South Africa' (2025) 7(3) *International Journal of Institutional Leadership, Policy and Management* 635-648.

Oyeniran L O, 'An Appraisal of Contemporary Issues in Trade Disputes Resolution in Nigeria' (2024) 6(1) *Kampala International University Law Journal* 1-22.

Ugonabo C, Nwoke F and Eze C, 'A Critical Review of Arbitration and Mediation Act 2023' (2026) 12(2) *Tropical Built Environment Journal* 9-22.

Wosu O G, 'The Procedures for Settlement of Trade Disputes in Nigeria' (2022) 6(2) *African Journal of Law and Human Rights* 45-65.

Statutes and Regulatory Instruments

Arbitration and Mediation Act 2023 (Nigeria).

Companies and Allied Matters Act 2020 (Nigeria).

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

Cybercrimes (Prohibition, Prevention) Act 2015 (as amended by Cybercrimes Amendment Act 2024) (Nigeria).

Evidence Act 2011 (as amended) (Nigeria).

Federal Competition and Consumer Protection Act 2018 (Nigeria).

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

Nigeria Data Protection Act 2023 (Nigeria).

Protection of Personal Information Act 4 of 2013 (South Africa).

Trade Act 2021 (United Kingdom).

Trade Disputes Act Cap T8 LFN 2004 (Nigeria).

UK Arbitration Act 1996 (as modernised by UK Arbitration Act 2025) (United Kingdom).

Judicial Decisions

Adene v Dantata (2003) 4 NWLR (Pt 811) 555.

Dickson v Sylva (2017) 8 NWLR (Pt 1567) 167.

Emma Elegbe & Anor v HP International Schools Limited & 3 Ors (2026) Supreme Court Decision SC/CV/123/2024.

Kubor v Dickson (2013) 4 NWLR (Pt 1345) 534.

Mix and Bake Flour Mill Ltd v National Union of Food, Beverage and Tobacco Employees (2012) 26 NLLR (Pt 73) 72.

Omisore v Aregbesola (2015) 15 NWLR (Pt 1482) 205.

Sahara Energy Resources Limited v Oyebola (2020) LPELR-51803(CA).

Sidumo v Rustenburg Platinum Mines Ltd (2007) 12 BLLR 1097 (CC).

Skye Bank Plc v Victor Anaemem Iwu (2017) 16 NWLR (Pt 1590) 24.

Suberu v African Petroleum Plc (2002) 7 NWLR (Pt 766) 244.

Western Steel Works Ltd v Iron and Steel Workers Union of Nigeria (1987) 1 NWLR (Pt 49) 284.

Internet Sources and Institutional Reports

Financier Worldwide, 'The UK Arbitration Act 2025: Key Changes and Summary Disposal' (August 2025) <financierworldwide/uk-arbitration-act-2025> accessed 14 August 2026.

International Chamber of Commerce (ICC), 'ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration' (2020) <arbitration-icca/cybersecurity-protocol> accessed 10 March 2026.

Kuti F, 'A Review of 2025 Significant Decisions in Labour and Employment Matters' (2025) <nicnadr/publications/kuti2025review> accessed 10 March 2026.

License(s): CC BY 4.0
See license terms at creativecommons.org
Downloaded from Global Insights Law Journal | gilawjournal.com

Pinsent Masons, 'England Cemented as Key Destination for Arbitration' (12 January 2025) <pinsentmasons/out-law/news/england-key-destination-arbitration> accessed 12 January 2026.

SimmonsCooper Partners, 'Employment and Defamation: Supreme Court Clarifies the Proper Forum for Workplace-Related Claims' (12 May 2026) <scp-law/employment-defamation> accessed 12 May 2026.

Downloaded from Global Insights Law Journal | gilawjournal.com

ARTICLE INFORMATION

A Legal Appraisal of Cybersecurity Challenges in The Resolution of Trade Disputes in Nigeria

Authors: Iwunze, Ireju Pamela

PUBLICATION
ISSN: 3141-5717 Volume: 1 Issue: 3 Publication Year: 2026

PERSISTENT DOI
https://doi.org/10.67588/0014

ARTICLE URL
https://gilawjournal.com/article/a-legal-appraisal-of-cybersecurity-challenges-in-the-resolution-of-trade-disp utes-in-nigeria

CITATION
Iwunze, Ireju Pamela, 'A Legal Appraisal of Cybersecurity Challenges in The Resolution of Trade Disputes in Nigeria' (2026) 1(3) Global Insights Law Journal. doi: 10.67588/0014

PUBLISHED BY

Global Insights Publishing

Official publisher of Global Insights Law Journal

PUBLICATION IMPRINT
Volume 1 | Issue 3 | Published 2026 | Editorial Office, Global Insights Law Journal | info@gilawjournal.com | gilawjournal.com

PUBLICATION LICENSE(S)
CC BY 4.0