Cybersecurity and Data Privacy Challenges in Nigeria's Digital Media Ecosystem

Dr. BABAJIDE Adeyinka Joseph
Department of Communication and Language Arts Education, College of Languages and Communication Arts, Lagos State University of Education, Oto/Ijanikin, Lagos State
Phone No.: 08033345456.
Email: babajideadeyinka@gmail.com

Plateau State University Journal of Communication Studies (PLASUJOCS) 2026, Vol. 3(1)

http://journals.plasu.edu.ng/index.php/pjcs

Abstract
This study investigated the vulnerabilities, regulatory hurdles, and structural threats facing users in the collection, processing, and protection of digital information within Nigeria's rapidly expanding online spaces. It explored how digital platforms balance the need for seamless information sharing with the need to prevent malicious attacks and safeguard user rights. Anchored by the Routine Activity Theory and Platform Governance, the study examined: dominant cybersecurity threats in Nigeria's online media; major data privacy concerns in the digital environment; adequacy of existing legal and institutional responses; implications for journalism, democratic communication, and public trust; and practical measures capable of strengthening platform resilience in Nigeria. The study adopted a qualitative critical review design, employing a systematic search strategy in accordance with PRISMA guidelines. This approach yielded an initial 200 records, from which 24 empirical and institutional documents were rigorously selected and evaluated using Braun and Clarke's thematic analysis framework. Guided by the four core objectives, the findings revealed that phishing, ransomware, and politically motivated disinformation are the dominant threat vectors, while opaque third-party tracking routinely violates user privacy. Also, the study discovered that these vulnerabilities systematically erode public trust and journalistic safety, simultaneously repudiating purely IT-centric paradigms of digital security. Furthermore, the analysis exposed a contradictory regulatory landscape where the Cybercrimes (Amendment) Act 2024 is frequently weaponised against journalists, undermining the progressive mandate of the Nigeria Data Protection Act (NDPA) 2023. The study concluded that digital vulnerabilities constitute a systemic crisis of communication governance rather than isolated technical failures. Consequently, it recommended that privacy-by-design be institutionalised, newsroom security protocols be comprehensive, advanced countermeasures, such as artificial intelligence, be deployed, and journalism be absolutely decriminalised to restore trust in Nigeria's digital media ecosystem.

Keywords: cybersecurity; data privacy; online media; platform governance; media ecology.

1. Introduction

The digital space in Nigeria has witnessed an increasing growth and a rapid development in the recent time. Interestingly, the country had 107 million internet users and 38.7 million social media user identities at the beginning of 2025 (Kemp, 2025). Messaging applications, social networking sites, online news platforms, streaming services, blogs and digital advertising systems have become central to everyday conversation, health education, political communication and mobilisation, commercial exchange and journalistic production. Although this expansion has widened access to information and public voice, it has also multiplied the scale of digital vulnerability (INTERPOL, 2025).

The failures of cyber-security in this environment do not merely compromise devices. They compromise newsrooms, sources, audience data, advertising accounts, reputational capital and public trust. Data privacy failures are equally consequential because they shape how citizens participate online, whether users can communicate without undue exposure, and whether platforms can be trusted with personal information.

Freedom House (2024) observed that Nigeria's internet environment remained

only partly free during the 2023-2024 coverage period, with online journalists still facing intimidation, legal prosecution and retaliation.

Much Nigerian scholarship has examined online fraud, misinformation, online journalism ethics or digital rights as separate themes (Apuke & Omar, 2021; Chiluwa, 2009; Hassan, 2023, Babajide, 2024). However, the present communication environment requires an integrated approach that links cyber threats, privacy governance, journalism and platform trust. It appears that the same platforms that carry legitimate reporting also host phishing messages, impersonation attempts, disinformation campaigns, abuse and unauthorised data extraction. It is against this background that this article pursues five related objectives: to identify the dominant cybersecurity threats affecting Nigeria's online communication and media platforms; to examine the major data privacy concerns in this digital environment; to assess the adequacy of existing legal and institutional responses; to discuss the implications of these

problems for journalism, democratic communication and user trust; and to propose practical measures capable of strengthening platform resilience in Nigeria.

2. Literature Review

The integration of digital technologies into Nigeria's media ecosystem has fundamentally transformed communication dynamics, creating a dual-use space characterised by democratic expansion and significant cyber-security vulnerabilities. Recent studies found that Nigeria possesses over 107 million internet users and nearly 39 million active social media identities (Kemp, 2025; Daodu & Babajide, 2024). This dense convergence of interpersonal messaging, citizen journalism, and professional news dissemination provides a fertile ground for digital threats. Viewed through the lens of Routine Activity Theory (Cohen & Felson, 1979; Yar, 2005), this rapid digital expansion has exponentially increased the number of "suitable targets" such as poorly secured newsrooms, media archives, and unencrypted journalistic sources, which make the entire ecosystem highly susceptible to malicious actors in the absence of capable guardianship.

Existing literature delineates a clear trajectory of cyber threats targeting the Nigerian digital space, evolving from basic digital financial deceptions (Chiluwa, 2009) to highly sophisticated attacks on institutional infrastructure and informational integrity. Threat vectors such as phishing, malware, and ransomware have become critically prevalent, frequently resulting in account takeovers and the severe disruption of media operations (ngCERT, 2024, 2025). Tade and Adeniyi (2020) argued that the persistence of these technical threats systematically erodes trust within the digital ecosystem. Beyond infrastructural attacks, the digital media ecosystem is heavily afflicted by cyber-enabled information disorders. Corroborating this position, Hassan (2023) and Igwebuike and Chimuanya (2021) demonstrated how misinformation and political disinformation thrive within this environment, exploiting platform algorithms and social tie strength. Conversely, the transformative potential of artificial intelligence in mitigating some of these challenges via minimising disinformation and fostering greater understanding has been highlighted as a necessary countermeasure in global and

local communication contexts (Babajide, 2024).

Data privacy in Nigeria's digital media landscape extends far beyond isolated corporate breaches to encompass the systemic extraction, surveillance, and monetisation of user data by platform operators. Apuke and Omar (2021) identified privacy invasion as one of the most prominent ethical challenges confronting online journalism in Nigeria, a problem exacerbated by media reliance on third-party digital trackers with opaque consent regimes. Furthermore, privacy concerns are inextricably linked to state surveillance and the physical and psychological safety of media practitioners. Uwalaka and Amadi (2023) highlighted how online harassment and digital surveillance have become normalised threat vectors against journalists, leading to institutional self-censorship and psychological fatigue. This environment underscores a critical digital vulnerability where platforms often fail to guarantee the anonymity, privacy, and safety required for independent journalistic practice.

The regulatory response to these cyber-security and privacy challenges reflects a complex, transitional, and often contradictory governance landscape. Aloamaka (2025) noted that the Nigeria Data Protection Act (NDPA) 2023 represents a significant institutional milestone, formally establishing robust principles of data minimisation, lawfulness, and institutional oversight. However, the application of broader frameworks, particularly the Cybercrimes (Amendment) Act 2024, remains highly contentious. Literature and empirical reports from digital rights organisations consistently point to the weaponisation of cybercrime provisions against journalists, whistleblowers, and critics (Committee to Protect Journalists, 2024; Freedom House, 2024; Reporters Without Borders, 2024). This paradox, where the state acts simultaneously as a statutory data protector and a potential threat to press freedom, highlights the inherent limitations of state-centric regulation and reinforces the necessity of adopting multi-stakeholder platform governance (Gorwa, 2019).

While substantial scholarship exists on isolated aspects of Nigeria's digital environment, including online fraud, fake news dissemination, and digital rights, there is a noticeable dearth of integrative research. Previous studies

have largely treated cybersecurity, data privacy, and journalism ethics as disparate fields of inquiry. A critical gap remains in examining how these elements intersect within a unified theoretical framework. By synthesising Routine Activity Theory and Platform Governance, this review establishes that technical vulnerabilities and regulatory enforcement cultures jointly shape the democratic utility of online platforms. Consequently, understanding this nexus is essential for proposing holistic measures that secure Nigeria's digital media ecosystem without compromising freedom of expression.

3. Methodology

This study adopted a qualitative critical review design, anchored in documentary analysis (Bowen, 2009). The study employed a transparent and systematic search strategy to select relevant documents, rather than relying on an ad-hoc literature gathering approach.

A systematic search strategy was deployed across primary academic databases including Scopus, Google Scholar, and Web of Science. The primary search terms included combinations of 'cyber-security', 'data privacy', 'online media', 'platform governance', and 'Nigeria'. To ensure relevance and contemporary applicability, specific inclusion and exclusion criteria were applied. Included documents had to be: (1) peer-reviewed academic articles, official government laws/advisories, or reports by recognised international digital rights organisations; (2) focused on the Nigerian digital or media context; and (3) published predominantly between 2015 and early 2026, though a few foundational earlier texts (e.g., Chiluwa, 2009) were retained for historical context regarding Nigerian cyber-fraud. Exclusion criteria eliminated opinion pieces, non-peer-reviewed commentaries, studies outside the Nigerian context, and articles lacking a clear focus on the media or communication ecosystem.

Based on these inclusion and exclusion criteria, the initial search yielded a total of 200 records (185 from academic databases and 15 from official institutional repositories). After removing 44 duplicates, 156 records were screened by title and abstract, leading to the exclusion of 112 irrelevant records. The remaining 44 full-text documents were assessed for eligibility, with 20 excluded for failing to meet the strict inclusion criteria such as lacking

specific media focus or insufficient empirical rigour. Ultimately, 24 documents (comprising peer-reviewed scholarship, official texts, and institutional reports) were included and used for the final thematic analysis. This selection process is visually detailed in the PRISMA flow diagram (Figure 1).

To analyse the data, the study utilised the six-phase framework for thematic analysis proposed by Braun and Clarke (2006). The included documents were read repeatedly, and data extracts were systematically coded. These codes were collated into potential themes, reviewed against the dataset, and ultimately defined under three primary analytical categories: threat patterns in the media ecology, privacy and surveillance vulnerabilities, and regulatory/institutional responses. This rigorous methodological approach ensured the study offers an evidence-based, logically sound, and transparent integration of existing knowledge.

Figure 1: PRISMA Flow Diagram for Systematic Document Selection

IDENTIFICATION Records identified through database searching (n = 185) Additional records identified through other sources (n = 15)	Records removed before screening: Duplicate records removed (n = 44)
SCREENING Records screened by title and abstract (n = 156)	Records excluded (n = 112)
ELIGIBILITY Full-text documents assessed for eligibility (n = 44)	Full-text documents excluded, with reasons (n = 20): - Lacked media/communication focus - Non-peer-reviewed commentaries - Focused outside Nigerian context
INCLUDED Studies included in qualitative synthesis and	

thematic analysis (n = 24)	

4. Data Analysis and Results

To directly address the core objectives of this study, the thematic analysis of the 24 included documents was structured into four distinct analytical categories. By triangulating data from peer-reviewed literature, institutional reports, and official advisories, this section provides comprehensive answers to the specific inquiries guiding the research.

4.1. Objective 1: Dominant Cyber-security Threats in Nigeria's Online Media

The first objective sought to identify the predominant cyber threats compromising online communication in Nigeria. The analysed data revealed that the digital media ecosystem is primarily targeted through four vectors: phishing, ransomware, account takeovers, and politically motivated disinformation. According to ngCERT (2025) advisories and INTERPOL (2025) threat assessments, phishing campaigns, targeting media professionals' credentials, have escalated, often exploiting the fast-paced nature of digital newsrooms. Explaining this trend, Routine Activity Theory posited that media archives and content management systems have become highly "suitable targets." Furthermore, the analysis highlighted a profound digital media effect where technical vulnerabilities overlap seamlessly with political communication. Apuke et al. (2024) and Hassan (2023) declared that misinformation and fake news are structurally enabled by these security flaws, allowing malicious actors to manipulate public discourse and severely distort the political communication environment.

4.2. Objective 2: Major Data Privacy Concerns in the Digital Environment

In addressing the second objective regarding data privacy, the documentary analysis uncovered systemic vulnerabilities rooted in the routine extraction and commercialisation of user data. Rather than spectacular, isolated data breaches, the primary concern lies in the opaque architecture of platform governance. Nigerian digital media platforms increasingly rely on third-party tracking tools, audience analytics, and algorithmic advertising models that operate without meaningful user consent. Apuke and Omar (2021) identified this invasion of privacy as a

central ethical crisis. The data suggested that audience information is routinely harvested to optimise digital advertising revenues, often at the expense of user anonymity. For investigative journalists and their sources, this lack of privacy-by-design poses an existential threat, as unencrypted communications and aggressive location tracking expose them to unwarranted surveillance.

4.3. Objective 3: Adequacy of Existing Legal and Institutional Responses

The third objective evaluated the sufficiency of Nigeria's regulatory frameworks in mitigating these digital threats. The findings indicated a contradictory institutional landscape. On one hand, the enactment of the Nigeria Data Protection Act (NDPA) 2023 represents a progressive step towards global standards, formally instituting the Nigeria Data Protection Commission (NDPC) to enforce data minimisation and lawful processing (Aloamaka, 2025). Conversely, enforcement data regarding the Cybercrimes (Amendment) Act 2024 reveals significant inadequacies. Reports from the Committee to Protect Journalists (2024) and Freedom House (2024) showed that instead of exclusively targeting cybercriminals, these statutory provisions are frequently used by state actors to prosecute journalists and stifle dissenting voices. This duality highlights a critical failure in platform governance, where the institutions mandated to act as "capable guardians" often exploit regulatory ambiguities to the detriment of digital rights and independent media.

4.4. Objective 4: Implications for Journalism, Democratic Communication, and Public Trust

Finally, the data was analysed to determine the broader implications of these vulnerabilities on the media ecosystem and public trust. The synthesis of the literature revealed profound negative effects on both democratic engagement and institutional reputational capital. Uwalaka and Amadi (2023) provided evidence that the normalisation of online harassment and state surveillance leads to psychological fatigue and self-censorship among media practitioners. When journalists cannot guarantee the confidentiality of their sources due to cyber vulnerabilities, the quality of investigative reporting inherently diminishes. Furthermore, from a corporate and institutional perspective, media organisations suffer severe reputational damage when their

platforms are compromised. As Tade

and Adeniyi (2020) observed in related digital sectors, repeated exposure to digital threats systematically erodes the "governance of trust." Ultimately, the analysis confirmed that cyber-security failures in Nigeria are not merely technical IT problems; they are systemic communication crises that degrade audience trust and threaten the foundational pillars of democratic communication.

5. Discussion of Findings

A critical synthesis of the results, guided by Platform Governance Theory, reveals a fundamental paradox in Nigeria's digital media ecosystem, in which the structural vulnerabilities of online platforms manifest simultaneously as technical failures and democratic crises. This study's findings significantly engage with existing scholarship, providing empirical corroboration for several contemporary assertions while challenging, and in some cases repudiating, narrower, purely technical paradigms of digital security.

Regarding the predominance of cyber threats in the media ecology (Objective 1), the findings strongly corroborate the conclusions of Hassan (2023) and Apuke et al. (2024) that misinformation and disinformation thrive precisely because of underlying platform vulnerabilities and social tie strengths. The escalation of phishing and account takeovers identified in this study align with early predictions by Chiluwa (2009) regarding the evolution of Nigerian cyber-deception, demonstrating a shift from basic financial fraud to the sophisticated manipulation of informational integrity. Furthermore, the demonstrated necessity for robust, systemic countermeasures corroborates Babajide (2024), who highlighted the critical need for advanced technological interventions, such as artificial intelligence, to mitigate digital disinformation and stabilise communication networks. However, this study strongly repudiates the traditional IT-centric view that phishing and ransomware are strictly isolated infrastructural problems. Instead, it establishes them as direct, systemic threats to political communication and media integrity.

In addressing data privacy (Objective 2), the study's findings corroborate Apuke and Omar (2021), who identified privacy invasion as a foundational ethical crisis in Nigerian digital journalism. Crucially, the current findings repudiate the dominant corporate narrative that

equates data privacy solely with the prevention of spectacular data breaches such as database hacking. Instead, the data reveals that systemic privacy degradation occurs through the routine, everyday architecture of platform governance, specifically through opaque third-party trackers and non-consensual audience analytics. This everyday surveillance creates a chilling effect on investigative journalism, corroborating Uwalaka and Amadi (2023) regarding the psychological fatigue and self-censorship induced by digital exposure.

Analysing the regulatory environment (Objective 3), this study corroborates Aloamaka (2025) in acknowledging the Nigeria Data Protection Act (NDPA) 2023 as a vital normative framework for establishing data minimisation and lawfulness. However, it strongly repudiates deterministic legal assumptions which posit that state-led cyber legislation automatically yields digital safety. By demonstrating the persistent weaponisation of the Cybercrimes (Amendment) Act 2024 against journalists, the findings align closely with the empirical reports of the Committee to Protect Journalists (2024) and Freedom House (2024). This corroborates Gorwa's (2019) Platform Governance Theory, illustrating that state actors in Nigeria often function simultaneously as statutory protectors of data and primary threats to journalistic freedom.

Finally, regarding the broader implications for public trust (Objective 4), the findings extend the arguments of Tade and Adeniyi (2020) beyond the financial sector to the media ecosystem. While Tade and Adeniyi found that digital fraud erodes trust in cashless systems, this study corroborates the view that similar digital vulnerabilities erode the "governance of trust" in online news platforms. The resultant loss of reputational capital and democratic participation reinforces the conclusion that cyber-security in Nigeria must be urgently reconceptualised as a core tenet of communication governance rather than a peripheral compliance issue.

6. Conclusion and Recommendations

This study has systematically examined the cyber-security and data privacy challenges within Nigeria's digital media ecosystem through the dual lenses of Routine Activity Theory and Platform Governance Theory. By critically synthesising 24 recent empirical and institutional documents, this research

concludes that digital vulnerabilities in Nigeria extend far beyond isolated technical IT failures. They constitute a systemic crisis of communication governance. The unchecked proliferation of phishing, ransomware, and state-enabled surveillance fundamentally erodes the reputational capital of digital platforms and the psychological safety of media practitioners. Furthermore, the paradoxical enforcement of the Cybercrimes (Amendment) Act 2024, in which state actors simultaneously regulate data and threaten press freedom, demonstrates that legislative existence does not equate to digital security. Consequently, mitigating these threats requires a paradigm shift from reactive technical patching to proactive, multi-stakeholder platform governance.

Based on the empirical findings and theoretical synthesis of this study, the following recommendations are proposed to safeguard Nigeria's digital communication environment:

1. Digital news platforms and platform operators must transition from opaque data extraction to privacy-by-design architectures. This requires strictly auditing third-party audience trackers and enforcing transparent, affirmative consent regimes for all users to prevent arbitrary surveillance.
2. To reduce the availability of "suitable targets," media organisations must mandate rigorous digital hygiene. This includes the mandatory use of end-to-end encryption for source protection, multi-factor authentication, and continuous incident-response training for all journalists.
3. State actors and law enforcement agencies must urgently cease the weaponisation of the Cybercrimes Act against media professionals. Statutory frameworks like the NDPA 2023 must be harmonised to protect freedom of expression as an indivisible component of national cybersecurity.
4. Media institutions and regulatory bodies should collaboratively explore the ethical integration of artificial intelligence to proactively detect and minimise disinformation campaigns, thereby stabilising the political communication environment.
5. Agencies such as the NDPC and ngCERT must transcend siloed operations by establishing active, continuous coordination with civil

society and media associations to foster comprehensive digital media literacy and ensure uniform compliance across the ecosystem.

Ultimately, restoring the "governance of trust" in Nigeria's online media space demands a holistic synthesis of robust technical safeguards, equitable legal enforcement, and the steady protection of democratic communication rights.

References

Aloamaka, P. C. A. (2025). A critical analysis of the Nigeria Data Protection Act 2023: Elevating standards to global norms. *UCC Law Journal, 4*(2), 242–263. https://doi.org/10.47963/ucclj.v4i2.1724

Apuke, O. D., & Omar, B. (2021). The ethical challenges and issues of online journalism practice in Nigeria: What do professionals and academics think? *Technology in Society, 67*, Article 101713. https://doi.org/10.1016/j.techsoc.2021.101713

Apuke, O. D., Omar, B., Tunca, E. A., & Gever, C. V. (2024). Does misinformation thrive with social networking site (SNS) dependency and perceived online social impact among social media users in Nigeria? Testing a structural equation model. *Journal of Asian and African Studies, 59*(1), 307–322. https://doi.org/10.1177/00219096221108738

Babajide, A. J. (2024). Transformative role of artificial intelligence in global communication: Minimising misinformation, disinformation, cultural diversity and fostering global understanding. *Lagos Journal of Contemporary Studies in Education, 2*(3), 33–44.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Chiluwa, I. (2009). The discourse of digital deceptions and "419" emails. *Discourse Studies, 11*(6), 635–660. https://doi.org/10.1177/1461445609347229

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Committee to Protect Journalists. (2024). *Nigeria police charge 4 journalists with cybercrimes for*

corruption reporting. https://cpj.org/2024/10/nigeria-police-charge-4-journalists-with-cybercrimes-for-corruption-reporting/

Daodu, M. A., & Babajide, A. J. (2024). Na(t)iveness of digital space: The consequentiality of media literacy and psycholinguistic approach for Nigerian university undergraduate students. In *Book of Proceedings 1st International Conference of College of Information and Technology Education (iCOITED 2024)* (pp. 171–183). Lagos State University of Education.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. Nigeria Data Protection Commission. https://ndpc.gov.ng/download/nigeria-data-protection-act-2023/

Federal Republic of Nigeria. (2024). *Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024*. WIPO Lex. https://www.wipo.int/wipolex/en/legislation/details/22699

Freedom House. (2024). *Freedom on the net 2024: Nigeria*. https://freedomhouse.org/country/nigeria/freedom-net/2024

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society, 22*(6), 854–871.

Hassan, I. (2023). Dissemination of disinformation on political and electoral processes in Nigeria: An exploratory study. *Cogent Arts & Humanities, 10*(1), Article 2216983.

Igwebuike, E. E., & Chimuanya, L. (2021). Legitimating falsehood in social media: A discourse analysis of political fake news. *Discourse & Communication, 15*(1), 42–58.

INTERPOL. (2025). *New INTERPOL report warns of sharp rise in cybercrime in Africa*. https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

Kemp, S. (2025). *Digital 2025: Nigeria*. DataReportal. https://datareportal.com/reports/digital-2025-nigeria

Nigeria Computer Emergency Response Team. (2024). *Escalation of*

ransomware attack in Nigeria. https://cert.gov.ng

Nigeria Computer Emergency Response Team. (2025). *Increase in phishing campaigns within the Nigerian cyberspace*. https://cert.gov.ng

Reporters Without Borders. (2024). *Nigeria: At least eight journalists prosecuted under cybercrime law despite new amendment*. https://rsf.org

Tade, O., & Adeniyi, O. (2020). Dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem. *International Journal of Offender Therapy and Comparative Criminology, 64*(16), 1717–1740.

Uwalaka, T., & Amadi, F. (2023). Beyond "online notice-me": Analysing online harassment experiences of journalists in Nigeria. *Journalism Studies, 24*(15), 1937–1956.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427.