



(RESEARCH ARTICLE)



REGULATING DEEPFAKES IN NIGERIA: ASSESSING THE ADEQUACY OF THE EXISTING CYBERCRIME FRAMEWORK

Ridwan Kolapo, Sarah Ousmane Yaye *, Samirah Usman, Sanusi Wakilat Olanrewaju, Babagoni Muhammad and Abdul-Shakur Sambo

Department of Information Technology, Nile University of Nigeria, Abuja, Nigeria.

* Corresponding Author

ORCID Details

Ridwan Kolapo: <https://orcid.org/0009-0005-9175-8195>

International Journal of Science and Research Archive, 2026, 21(01), 324–330

Publication history: Received on 03 September 2026; revised on 10 October 2026; accepted on 12 October 2026

Article DOI: <https://doi.org/10.30574/ijrsra.2026.21.1.1878>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Generative artificial intelligence now enables the cheap fabrication of audio, images and videos of real people. Nigeria has been the scene of a range of such abuse, from a cloned-voice clip preceding the 2023 elections to deepfakes of the President and of Peter Obi from 2024 to 2026. This article examines the adequacy of Nigeria's cybercrime law to regulate deepfakes, based on four stages of their life: acquisition, synthesis, dissemination and consequence and four criteria of evaluation: rule clarity, institutional responsibility, enforceability and remedy. Using a qualitative doctrinal method, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended in 2024), the Nigeria Data Protection Act 2023, the Evidence Act 2011 (as amended 2023) and constitutional privacy are evaluated for application to deepfakes. The cybercrime law covers fraud, impersonation and child sexual abuse imagery deepfakes, and (arguably) sexual deepfakes, but offers no definition of synthetic media, no offence of non-consensual synthesis (or of possession/distribution of synthetic media), no takedown duty for deepfakes, and no rules or capacity for authenticating electronic evidence. Statutory reform is recommended, focused narrowly on the regulation of deepfakes, including through labeling duties, victim-focused remedies, forensic capacity-building and harmony with national-level AI governance.

Keywords: Deepfakes, Synthetic media, Cybercrime, Data protection, Law.

1 INTRODUCTION

The emergency of generative intelligence has significantly lowered the technical barriers previously associated with creating convincing recordings of real individuals. While fabricating such recordings ones required considerable skill, time and specialized equipment, generative AI now enables the production of synthetic audio, images and videos that can convincingly depict real people saying or doing things they never said or did. Such manipulated media are commonly referred to as deepfake [1]. In Nigeria, experts have reported that ordinary citizens may struggle to distinguish hyper-realistic synthetic voices and videos from authentic recording [2].

Nigeria has not been spared the deluge; a clip purporting to capture Atiku Abubakar, Ifeanyi Okowa and Aminu Tambuwal discussing how to rig the vote was disseminated before the 2023 presidential election; fact-checkers uncovered unnatural features indicating that the voices were AI-generated [2]. In 2024, a video purported to show President Tinubu speaking about buying the Chelsea Football Club, which he never said; in May 2025, a 49-minute video purported to show Peter Obi addressing the leader of Burkina Faso had more than 136,000 views through to late June; Dubawa later revealed that manipulated audio had been layered over genuine footage [3]. In May 2026, the Presidency warned that deepfake videos and manipulated audio were being used against the President before the 2027 elections [4]. The damage is not limited to the political sphere: reporting also reveals Nigerian users fabricating sexually explicit deepfakes of women without consent [3].

Nigeria has no statute written for deepfakes, or for artificial intelligence generally [5], any response must be built from general law, specifically the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and its 2024 Amendment Act. This article asks: is the existing cybercrime framework, read with the data-protection, evidence and constitutional rules surrounding it, adequate to regulate deepfakes? We argue that coverage is real but partial; it is strongest where a deepfake is a tool of fraud, and weakest where a person's likeness is synthesized without consent and where courts must judge what is authentic.

2 LITERATURE REVIEW

2.1 Concept and harms

Academics view deepfake as a multifaceted legal conundrum that attracts myriad of challenges relating to disinformation. Indeed, [1] posit that using this software could cause the creation of deceptive information and interference with elections, production of fabricated evidence in courts of law, and non-consensual imagery synthesis where the legal implications depend on the mode of use or production, not the technology itself. This observation provides a theoretical backing to the consequentialist approach to deepfake regulation that focuses on the harms in context rather than the technology as the main vantage point of analysis. Nigerian studies and reports have identified some of the key challenges attributed to deepfake technology use in the country including political disinformation, impersonation fraud, image-based sexual assault, and a general mistrust of evidence [3],[6],[5].

2.2 Nigerian scholarship on Deepfakes and Legal Regulations

Nigerian writing concurs on the main diagnosis. [5] observes that the response is fragmented: there is no statute dedicated to regulating deepfakes, and protection is scattered across different data-protection, copyright, image-rights and defamation law frameworks, with gaps surrounding AI training data, non-consensual intimate imagery and algorithmic transparency. [6] describe a serviceable but incomplete patchwork appropriate for "a world of forged documents and stolen passwords" but not "fabricated faces and cloned voices". Practitioners concur: [7] finds no provision dedicated to deepfakes and concludes that such conduct should be treated as a variation of existing offenses. [8] link deepfakes to cyber-violence and propose comprehensive legislation and new criminal laws, but they wrote the piece prior to the Nigeria Data Protection Act 2023 and the 2024 amendment to the Cybercrimes Act. On that amendment, the Lex Initiative for Rights Advocacy and Development in 2025 welcomes the narrower section 24 but warns that its higher threshold may leave some harassing, non-threatening conduct outside the offence.

2.3 Comparative approaches

Comparative practice offers two models. The first is transparency. Article 50 of the European Union's Artificial Intelligence Act requires providers to mark synthetic output in machine-readable form and deployers to disclose synthetic content to the public, with fines of up to €15 million or 3% of worldwide turnover; the duties began to apply on 2 August 2026 [9].

The second is targeted prohibition. The United States' TAKE IT DOWN Act criminalizes publishing non-consensual intimate imagery, including AI-generated imagery, and since 19 May 2026 requires covered platforms to remove it within 48 hours of a valid request [10], [11]. Targeted rules can still fail on speech grounds: a federal court struck down California's election-deepfake statute AB 2839 in 2025 because it was not narrowly tailored [12]. The common lesson is to define the harmful conduct precisely, rather than to ban generative technology.

3 RISKS OF DEEPPAKES IN NIGERIA

The incidents in Section 1 (*Political disinformation*) show deepfakes entering politics before elections, mixing synthetic voices with real footage. Fact-checkers say misinformation travels faster than their corrections, and that voters can spot simple photo edits but struggle with synthetic audio and video [2]. The Independent National Electoral Commission (INEC) created an Artificial Intelligence Division in May 2025, with a mandate that includes fighting disinformation [2].

The same report noted that Nigeria’s legal and policy systems had not yet adapted to election-related AI misuse. The Electoral Act 2022 on which it commented has since been repealed and re-enacted as the Electoral Act 2026 [13].

[5] documents synthetic media used to defraud consumers (*Fraud and impersonation*), and [6] treat impersonation as a distinct legal front. *Image-based sexual abuse*. A 21 Magazine investigation reported by TheCable describes users creating sexually explicit deepfakes of women without consent [3]. The Nigeria Data Protection Commission (NDPC) and more than 60 other data-protection authorities have warned that such tools enable defamatory content and non-consensual intimate imagery, with particular risks for children and other vulnerable groups [18].

Trust in audio and video is high and digital literacy is uneven (*Structural conditions*), especially in rural areas [2], [3]. Detection tools exist, but fact-checkers say none is fully reliable, and groups such as Dubawa train journalists to spot deepfakes manually [2], [3]. When the Obi video was reported on, it remained online, untouched by platform moderation or takedown [3].

4 LEGAL AND CONCEPTUAL FRAMEWORK

4.1 The Cybercrimes Act 2015, as amended in 2024

The Act makes no mention of deepfakes, synthetic media or artificial intelligence. It covers these activities, if at all, through technology-neutral crimes. Table 1 below indicates the relevant provisions.

Table 1: Provisions of the Cybercrimes Act most relevant to deepfakes

Provision	How it may apply to a deepfake	Main limit
s. 13 Computer-related forgery	Altering or fabricating computer data (audio, image or video files) so that it is acted on as authentic.	Needs intent that the data be treated as genuine; weak fit for satire or fakes not used to deceive a recipient.
s. 14 Computer-related fraud	A cloned voice or face used to induce a transfer of funds or property.	Needs fraud and loss; does not reach non-financial deepfakes.
s. 22 Identity theft and impersonation	Dishonest use of another person’s unique identification feature, or impersonation to gain an advantage, obtain property or disadvantage the person impersonated.	Drafted around credentials and financial fraud; whether a face or voice is a “unique identification feature” is untested.
s. 23 Child pornography	Realistic images of a minor in sexually explicit conduct are expressly covered, so AI-generated child abuse imagery is caught.	Child imagery only; nothing equivalent for adults.
s. 24 Cyberstalking (as amended)	Sending a pornographic message, or a message the sender knows to be false and sends to cause a breakdown of law and order or threaten life.	“Pornographic” is undefined and consent-blind; political deepfakes are caught only if the stated purpose is proved.

The most significant provision is Section 24, which is the most used one. Before 2024 it covered messages that contained grossly offensive or menacing words, or that were known to be false and sent to cause annoyance or needless anxiety. The ECOWAS Court found it vague and unlawful and civil society campaigned for its amendment [15]. The 2024 Amendment Act narrowed it down to messages that are pornographic, or that the sender knows to be false and sends to cause a breakdown of law and order or threaten life. Critics argue that “breakdown of law and order” is undefined and that journalists are still being arrested under this section [16].

4.2 The Nigeria Data Protection Act 2023

The NDPA regulates the processing of personal data and treats genetic and biometric data processed to identify a person uniquely as sensitive personal data, which requires stricter grounds such as explicit consent [17]. A face or voice used to train or generate a deepfake may be regarded as personal data. Two limitations follow. Biometric data is sensitive only when processed to identify someone, and the Act is designed to regulate organizations that control or process data, not anonymous individuals. In February 2026 the NDPC joined 60 other authorities in a statement expecting safeguards, transparency and rapid removal mechanisms from AI image-generation systems [18]. This is a statement of regulatory expectations, not a deepfake offence.

4.2.1 Prohibitions & Deepfake Coverage

The NDPA forbids processing sensitive personal data without the data subject's permission or a lawful basis for processing. As such, using someone's face or voice to train, tune, or create an unauthorized deepfake is a prohibited data processing activity.

4.2.2 Limitations & Uncertainties

There are two major loopholes in the efficacy of the Act against deepfakes:

- The Identification Loophole: Since Biometric information is only considered "sensitive" when processed for identification, if a creator processes someone's biometric for creating a likeness or parody, it leaves ambiguity about the applicability of Section 30.
- The Target Limitation: As the Act is explicitly geared towards regulating formal organizations (data controllers and processors), it cannot punish independent digital creators or anonymous individuals who produce deepfakes.

4.3 The Evidence Act 2011, as amended in 2023

Section 84 deals with the admissibility of computer-generated evidence. The Evidence (Amendment) Act 2023 widened the scope of this section to include "electronic records" [19], and the Supreme Court has directed strict compliance with the requirements set out in this section [20]. These requirements relate to how the electronic record is generated, specifically, that the computer was in regular use and that information was regularly supplied to it. The section focuses on the machine and its regularity, not on the contents of a computer record or its ability to demonstrate that a certain event took place.

4.4 Constitutional privacy and image rights

Section 37 of the Constitution safeguards privacy, but no court has built a general deepfake remedy from this right. More relevant is [21], where the Nigerian Supreme Court ruled that a claim for unauthorized commercial use of one's image does not amount to copyright infringement; rather, it is an action that can be heard in the State High Court because image rights or personality rights are distinct from copyright [7]. [5] draws on this case in the deepfake context.

5 ANALYSIS AND DISCUSSION OF FINDINGS

5.1 Acquisition

Here the NDPA is the only relevant instrument. Collecting photographs or voice recordings from social media to model a particular person can be processing of personal data which requires a lawful basis of processing, and the sensitive-data rules apply where biometric data is processed for the purpose of identifying [17]. The public availability of an image does not per se authorize every single use. However, whether private individuals acting alone are caught depends on the purpose and context of their processing, and the NDPC's attention so far is being focused on organizations [18]. The rule is reasonably clear for organizations and an institution is identifiable, but enforcement against anonymous individuals is hard, and the remedies are largely administrative.

5.2 Synthesis

This is the most apparent loophole. The offenses in Table 1 apply only to what the offenders intend to achieve through the reproduction such as fraud, forgery, impersonation for economic or social advantage, or causing public order impediment. None of them make it an offence per se to create a realistic image of an identifiable adult without consent. At the same time, an intimate image can damage one's dignity even before it is shared. Only section 23 explicitly address synthetic imagery, albeit exclusively in the context of children. [5] notes that non-consensual intimate imagery is a regulatory gap, and Lex Initiative for Rights Advocacy and Development in 2025 highlights the risk that narrowing the scope of section 24 creates for various forms of harassment not being covered by the law.

6 DISSEMINATION

The existing law bites hardest here, but unequally: financial deepfakes fit reasonably well into sections 14 and 22 so long as intent to defraud is proved. A sexual deepfake that is sent or posted may fall within the pornographic limb of section 24, though that term is undefined and the section not written around consent. Political deepfakes are less clear. After the 2024 amendment, a deepfake of a candidate is caught by section 24 only if the sender knows it is false and sends it to cause a breakdown of law and order or threaten life. Those intended solely to damage a reputation or mislead voters without that purpose fall outside the section, and have to find support in defamation or the Electoral Act, which were not

written for synthetic media [2]. But at the same time, the vagueness of “breakdown of law and order” leaves the same section open for use against journalists and critics [16]. The framework is thus both under- and over-inclusive. The NDPA and the Act contain nothing approaching the notice-and-removal duties of the TAKE IT DOWN Act for deepfakes, and the Obi video remained online [3].

Consequence and remedies

A victim typically has the four pressing needs that include preservation of the original material, removal, correction, and protection from further harassment. The existing law provides a mosaic. Prosecution requires identification of the offender, a complaint to the NDPC is typically more effective against organizations, and a civil action under *Ubom* will help if the offending image has been used to market a product, in the case of a spoof endorsement, but less clearly if the harassment is non-commercial, such as a sexual or political deepfake. There is no single remedy that will provide a link between preservation, takedown, investigation and redress, and so the victim must determine which of several possible options to pursue.

6.1 Evidence and authentication

A deepfake may be generated on a properly functioning computer, stored in a standard format and presented with a certificate that satisfies section 84, since the conditions test production, not truth. Courts therefore must distinguish between the provenance of a file and the accuracy of the images that the file depicts. The reverse danger is also present: genuine recordings may be dismissed as fabrications merely because their manipulation is possible, and [1] warn that deepfakes threaten the reliability of evidence in court. We identified no provision empowering Nigerian courts to order forensic authentication where manipulation is credibly alleged.

6.2 Enforcement capacity

Fact-checkers have already deployed detection tools. However, they acknowledge the limitations of these tools and complement them with manual verification [2], [3]. If specialist fact-checkers face these limits, the police and courts are likely to face them too, so statutory reform without forensic capacity will leave new offenses hard to enforce.

6.3 Summary of findings

Table 2 summarizes the assessment of our criteria. It is a qualitative judgement, not a quantitative one.

Table 2: Adequacy of the existing framework by stage

Stage	Clear rule?	Responsible institution?	Enforceable?	Remedy?
Acquisition	Partly (NDPA; organisations)	Yes (NDPC)	Weak against individuals	Administrative
Synthesis	No	Unclear	Weak	None specific
Dissemination	Partly (fraud, s. 24, s. 23)	Police and courts; platforms unclear	Moderate if the offender is identified	Criminal penalties; no takedown duty
Consequence	Fragmented	Several, uncoordinated	Weak	Fragmented (criminal, NDPC, civil)
Evidence	No	Courts	Weak (forensic capacity)	Not addressed

Five issues stand out. Firstly, Nigeria is not a legal vacuum; there are points of intervention in existing cyber-crime, data-protection, privacy and evidence legislation. Secondly, coverage seems to depend on the intention of the offender, so that similar synthetic acts may be differently covered. Thirdly, the framework is weakest in the area of non-consensual synthesis and in the area of authentication. Fourthly, the question of capacities and coordination is as important as statutory wording. And finally, the history of section 24 shows the need for caution in the drafting of any new offence.

7 CONCLUSION AND RECOMMENDATIONS

In order to fill the regulatory gaps that have been identified in the study, Nigeria needs to shift from the reactive, outdated laws to the proactive and coherent approach. Below are the suggested changes that may be taken to regulate

deepfakes in the country, outlining the necessary amendments, obligations, and collaboration between government and private entities.

- *Define and target*: amend the Cybercrimes Act to define “synthetic media” and “deepfake” and to target narrow offenses of non-consensual sexual deepfake, malicious synthetic impersonation, and deceptive election deepfake within a defined period, each requiring intent and serious harm to individuals, with express exceptions for satire, parody, journalism and research, replacing the vague “breakdown of law and order” test.
- *Require transparency*: obligate AI providers and major platforms operating in Nigeria to mark synthetic output and disclose deepfakes (adapting Article 50 of the EU AI Act) with a phase-in under a designated regulator such as NITDA.
- *Build a victim pathway*: a reporting/preservation channel, a notice-and-removal procedure with verification and appeal, and a civil remedy building on *Ubom* and image rights.
- *Reform evidence practice*: allow courts to order forensic authentication where manipulation is credibly alleged, distinguishing the provenance of a file from the truth of its content.
- *Fund capacity*: provide forensic tools and training for the police, other investigating agencies and the judiciary, while supporting fact-checkers, including detection tools working in Nigerian languages.
- *Coordinate and integrate*: ahead of the 2027 elections, INEC, NITDA, the NDPC, the police and the Cybercrime Advisory Council should agree on a joint protocol on election deepfakes. Deepfake policy should be nested within national AI governance (Federal Ministry of Communications, Innovation & Digital Economy, 2025) and supported by public digital literacy programmes.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

No conflicts of interest regarding this manuscript.

REFERENCES

- [1] Van der Sloot B, Wagenveld Y. Deepfakes: regulatory challenges for the synthetic society. *Comput Law Secur Rev.* 2022 Sep;46:105716. doi:10.1016/j.clsr.2022.105716.
- [2] TechCabal. Road to 2027: preparing for Nigerian elections in a world of AI deepfakes [Internet]. 2025. Available from: <https://techcabal.com/2025/08/28/ai-deepfakes-nigeria-2027elections/>
- [3] Emudianughe PO. The rise of deepfakes and the fight for digital truth [Internet]. TheCable Fact Check. 2025. Available from: <https://factcheck.thecable.ng/the-rise-of-deepfakes-and-the-fight-for-digital-truth/>
- [4] TheCable. Presidency: desperate actors using deepfake video for anti-Tinubu religious propaganda [Internet]. 2026. Available from: <https://www.thecable.ng/?p=1338160>
- [5] Owoade AO. Deepfakes in Nigeria: a fragmented legal and regulatory landscape for synthetic media [Internet]. SSRN; 2026. doi:10.2139/ssrn.7378019.
- [6] Nduka RE, Nduka CV. Deepfakes, artificial intelligence and Nigerian law: is the law ready for synthetic reality? *Afr J Law Ethics Educ.* 2026;9(7):1-18. Available from: <https://ajleejournal.com/index.php/ajlee/article/view/422>
- [7] Olisa Agbakoba Legal. Review: *Ubom v GlobalCom (Nig.) Ltd* (2025) 6 NWLR (Pt 1985) 157 @ 183 [Internet]. 2025. Available from: <https://oal.law/review-ubom-v-globalcom-nigltld-2025-6-nwlr-pt-1985-157-183/>
- [8] Ibrahim AM, Jamri B, Zakari A. Implications of artificial intelligence-driven deepfakes for cybersecurity and regulation in Nigeria: theorising for cyberfakes and cyberviolence. In: Francia G III, Zanzig JS, editors. *Global perspectives on information security regulations: compliance, controls, and assurance*. Hershey (PA): IGI Global; 2022. p. 185-221. doi:10.4018/978-1-7998-8390-6.ch008.
- [9] Goodwin Procter LLP. Not delayed, not deferred: EU AI Act transparency obligations are now in force [Internet]. 2026. Available from: <https://www.mondaq.com/uk/compliance/1826042/not-delayed-not-deferred-eu-ai-act-transparency-obligations-are-now-in-force>
- [10] United States Congress. TAKE IT DOWN Act. Pub L No. 119-12. 2025. 139 Stat 55.
- [11] The TAKE IT DOWN Act goes live [Internet]. WilmerHale. 2026. Available from: <https://www.wilmerhale.com/en/insights/client-alerts/20260615-the-take-it-down-actgoes-live>

- [12] Kohls v Bonta. 797 F Supp 3d 1177 (ED Cal 2025).
- [13] Electoral Act, 2022. Abuja: Federal Republic of Nigeria; 2022. Repealed by the Electoral Act, 2026.
- [14] Electoral Act, 2026. Act No. 1 of 2026. Abuja: Federal Republic of Nigeria; 2026.
- [15] Paradigm Initiative. Press release: coalition lauds Cybercrimes Act amendment and urges FG to further safeguard freedom of expression [Internet]. 2024. Available from: <https://paradigmhq.org/press-release-coalition-lauds-cybercrimes-act-amendment-and-urges-fg-to-further-safeguard-freedom-of-expression/>
- [16] Nnochiri I. What is the cost of freedom of expression [Internet]. Vanguard News. 2026. Available from: <https://www.vanguardngr.com/2026/09/what-is-the-cost-of-freedom-of-expression/>
- [17] Nigeria Data Protection Act, 2023. Abuja: Federal Republic of Nigeria; 2023.
- [18] Nigeria Data Protection Commission. Joint statement on AI-generated imagery and the protection of privacy [Internet]. Abuja: Nigeria Data Protection Commission; 2026 Feb 23. Available from: <https://ndpc.gov.ng/joint-statement-on-ai-generated-imagery-and-the-protection-of-privacy-23-february-2026/>
- [19] ALN Nigeria. Highlights of the Evidence (Amendment) Act 2023 [Internet]. Lagos: ALN Nigeria; 2023. Available from: <https://aln.africa/insight/highlights-of-the-evidence-amendment-act-2023/>
- [20] Kubor v Dickson. (2013) 4 NWLR (Pt 1345) 534 (Supreme Court of Nigeria).
- [21] Ubom v Globacom (Nig.) Ltd. (2025) 6 NWLR (Pt 1985) 157 (Supreme Court of Nigeria).