Who is Liable for a Deepfake? A Comparative Analysis of Creator, Distributor, and Platform Responsibility Under Nigerian Law

Ridwan Kolapo, Oluwatobi Kuye, Olorunshola Raphael Ajayi, Ogonnaya Onwuchekwa, Taheer Abubakar Kawu, Andrew Warebi Denyan

Department of Information Technology, Faculty of Computing, Nile University of Nigeria.

DOI: https://doi.org/10.47772/IJRISS.2026.100900730

Received: 03 October 2026; Accepted: 08 October 2026; Published: 22 October 2026

ABSTRACT

The increasing accessibility and sophistication of generative artificial intelligence have made deepfakes easier to produce and disseminate, creating significant legal challenges concerning accountability for synthetic media. Although Nigeria has laws addressing cybercrime, data protection, privacy, and related harms, it lacks a legal framework specifically tailored to deepfakes. This article examines the extent to which existing Nigerian law addresses the liability of three principal actors in the deepfake production and distribution chain: creators, distributors, and online platforms. Using doctrinal and comparative legal analysis, the study evaluates relevant Nigerian legislation and compares the domestic framework with approaches adopted in the European Union, the United Kingdom, and the United States. It applies a layered analytical framework based on knowledge, intent, and control to assess the responsibility of each actor. The findings indicate that Nigerian law can address creators' conduct through existing cybercrime and data protection provisions, although the absence of deepfake-specific offenses creates challenges in addressing distinctive forms of harm. Distributors may incur civil liability where the requisite knowledge and other legal elements can be established, but evidentiary difficulties complicate enforcement. Online platforms, meanwhile, are subject to reactive notice-and-takedown obligations under Nigeria's regulatory framework, with limited proactive duties specifically addressing deepfake-related risks. The comparative analysis considers the European Union's Artificial Intelligence Act, the United Kingdom's Online Safety Act 2023, and the United States' TAKE IT DOWN Act. The article recommends introducing a specific deepfake offence within Nigeria's cybercrime legislation, strengthening proactive platform risk-mitigation duties, establishing time-bound takedown requirements for non-consensual intimate imagery, and providing appropriate safeguards for satire and parody. It concludes that effective deepfake governance in Nigeria requires clearer legal standards, improved enforcement, and a balanced approach that protects individuals from harm without unduly restricting freedom of expression.

Keywords: Deepfakes, Cybercrime, Creator Liability, Distributor Liability, Platform Liability, National Information Technology Development Agency (NITDA).

INTRODUCTION

Despite their use in satire, entertainment, marketing and other forms of digital expressions, deepfakes have emerged as a significant legal and societal concern due to the increasing difficulty of distinguishing AI-generated content from authentic audio, images and videos. Advances in generative artificial intelligence have made it increasingly easy to create highly synthetic representation of real individuals, thereby expanding both the legitimate and harmful uses of deepfake technology. While deepfakes may serve creative and communicative purposes, they can also be exploited to facilitate fraud, impersonation, political manipulation, reputational harm and sexual abuse. (Mustak et al., 2023; Whittaker et al., 2021). Their threat has partly to do with scenarios that are out of human reach, as experimental research has already demonstrated that humans are not yet able to be certain whether the deepfakes are real or fake, but they can still be certain that they are fake (Köbis et al., 2021). Deepfakes are thus not just a problem for the victim, but for many others. They diminish trust in audiovisual evidence (Fallis, 2021; Aylett et al., 2023) and may negatively impact fundamental democratic roles (Pawelec, 2022; Łabuz & Nehring, 2024).

During the 2023 general elections, deepfakes, a term describing manipulated or synthetically generated images, videos, and audio recordings which have been manipulated to present agenda-driven propaganda were common on social media with the aim of smearing electoral contestants and disseminating propaganda (Ekpang, Iyorza & Ekpang, 2023). Nigeria's Data Protection Commission has also acknowledged the risk when it, along with over sixty data protection authorities, issued a warning earlier in 2026 against AI systems that are able to create realistic images and videos of identifiable individuals without consent (Nigeria Data Protection Commission, 2026). But Nigeria does not have a law specifically geared towards deepfakes. This has resulted in what is often described as a patchwork legal framework for online defamation, privacy and data protection, impersonation, cybercrime, evidence just to mention some, which were also highlighted by commentators in the legal framework of the country as a deficit on its own (Olisa Agbakoba Legal, 2021; Alabi, 2025).

An important question raised by this gap is, who should be responsible if a deepfake is harmful? Deepfakes typically involve several actors in their creation and dissemination. It goes through a series of actors, the actor that creates it, and the people that distribute it, and its online platforms that host and amplify it. No single one of the participants is in charge of the entire process (Chesney & Citron, 2019). All actors are also distinct in terms of their knowledge and intent. Creators typically make decisions on a purposeful basis, while malicious creators are most unlikely to adhere to labeling requirements (Łabuz, 2023). Many distributors, on the other hand distribute deepfakes unwittingly and different factors such as political interests, cognition, and network size influence who distributes them (Ahmed, 2021). Responding to harmful effects, rather than responsibility, platforms have largely set aside the funding of detection research. Instead, platforms have mainly dedicated resources to detection research rather than accepting responsibility for harm (Vizoso et al., 2021).

Mixed lessons are also provided by other jurisdictions. The EU AI Act has obligations for transparency when it comes to deepfakes, but with a limited effect (Łabuz, 2023). The UK Online Safety Act has been criticized for its lack of consistency in platform policies, as well as for its delayed content removal (Kira, 2024). From a comparative perspective, the EU, US, UK and China show the need for Content Provenance Standards, explainable detection techniques, and harmonized rules (Romero-Moreno, 2025). Others point out that the impacts of deepfakes are largely reinforcing the negative effects of 'real' fakes, making the enforcement of existing laws potentially as important as introducing new preventive legislation (Birrer & Just, 2025). Furthermore, though African legal systems are seldom studied by scholars, research on this issue in Nigeria is scarce (Ekpang, Iyorza & Ekpang, 2023).

LITERATURE REVIEW

Responsibility of developers and distributors

In the literature, the distinction between creators and distributors is based primarily on know-how and purpose. Creators may act with varying degrees of intent and accountability, which is why malicious creators do not adhere to transparency obligations, such as those under the EU AI Act, labeled creator information must be included (Łabuz, 2023). Gaps have been identified in Indonesia as described by Meliala and Utari (2026), who recommend for the enactment of laws that explicitly punish the creation and dissemination of deepfakes. Distributors face a more difficult question with many people making the deepfakes without realizing. Short of certainty, they are able to detect deepfakes, but think they are better at than they actually are (Köbis et al., 2021) and political interests, cognitive skills and network size dictate whom they might be shared with unintentionally (Ahmed, 2021). Making all sharers liable would have the effect of punishing an error most would make, and not coming to grips with the concept of holding all sharers liable would do nothing to combat virus spreading. The literature, thus suggests a knowledge based standard, but there are only rare texts indicating such a standard.

Responsibility of online platforms

Responses from platforms were initially voluntary and included funding detection research (Vizoso et al., 2021). Since then, the effectiveness of self-regulation has been called into question. Kira (2024) states inconsistent platform policies and after-the-fact removal, especially of intimate deepfakes, are key failures of the UK Online Safety Act. Chesney and Citron (2019) address the issue at the broadest level, that of the entire chain of creation

and dissemination, also observing that neither an actor liability nor a platform liability doctrine can fix the problem alone.

Technical and legal solutions

Regulatory approaches vary, it could be subject of data protection reforms and ex ante restrictions on the distribution of deepfake technology (van der Sloot & Wagensveld, 2021). Among the options compared by Romero-Moreno (2025) are the implementation of standards for provenance, explainable AI, and harmonized rules. Others suggest turning to deepfake laws under international law (Kuźnicka-Błaszkowska & Kostyuk, 2025). Regardless, detection is primarily powered by deep learning (Rana et al., 2022), but cannot be afforded due to the rapid pace at which generation is occurring, while coordinated response among firms, regulators and users (Mustak et al., 2023) is needed for effective mitigation.

The Nigerian Case and the Gap in Literature

There have been limited studies done in Nigeria. In the 2023 elections, Ekpang, Iyorza and Ekpang (2023) reported the spamming of candidates, especially from the aspect of images and voice and the lack of robustness in Nigeria's electoral laws to handle synthetic media was found by commentary (Olisa Agbakoba Legal, 2021; Alabi, 2025). The studies considered most relevant to this paper are summarized in Table 1.

Table 1. Summary of key studies on deepfake liability.

Author (Year)	Method	Problem addressed	Key findings	Limitations
Olisa Agbakoba Legal (2021)	Legal commentary	Adequacy of Nigerian law for deepfakes	Framework is an incomplete patchwork; reform needed	Practitioner commentary, not peer-reviewed
Ekpang, Iyorza & Ekpang (2023)	Survey of 1,123 respondents	Deepfakes in Nigeria's 2023 elections	Used to smear candidates and spread propaganda	One region; self-reported data
Chesney & Citron (2019)	Doctrinal-comparative analysis	Liability across a chain of actors	Identifies the actor-chain problem; no single actor controls the process	US-centric; predates EU AI Act
Łabuz (2023)	Legal analysis of the draft AI Act	Adequacy of deepfake transparency rules	Malicious creators evade labelling duties	Analyzed the draft, rather than the final Act
Ahmed (2021)	Survey	Who shares deepfakes unknowingly	Political interest, cognitive ability and network size matter	Self-reported; cross-sectional
Köbis et al. (2021)	Behavioral experiments	Human detection ability	Poor detection ability accompanied by overconfidence	Lab stimuli
Vizoso et al. (2021)	Comparative case study	Media and platform responses	Platforms fund detection research	Six organizations only
Kira (2024)	Legal and policy analysis	UK Online Safety Act and intimate deepfakes	Relies on weak platform policies and late removal	UK-specific
Romero-Moreno (2025)	Comparative legal and technical analysis	Detection laws across EU, US, UK, China	Recommends provenance standards and harmonized rules	No African jurisdictions
Birrer & Just (2025)	Systematic review and policy analysis	State of evidence and regulation	Deepfakes amplify existing harms	Thin empirical base

From Table 1 above three major gaps emerge, firstly, there is no mention of the laws of Africa when compared with those of the EU, US and UK, or China, regardless of the extent of their repercussions on Africa as sites of

liability. Only a limited focus on Africa in its laws is sufficient for the discussion of the processes of wide reaching repercussion (Romero-Moreno, 2025). Secondly, no Nigerian study distinguishes between the role of the creators, distributors and platforms separately (Ekpang, Iyorza & Ekpang, 2023). Third, there is no liability standard distinction between knowing and unknowing distribution (Ahmed, 2021; Köbis et al., 2021).

Assessing the Risk and/or Liability for Each Actor

This section applies a layered framework to the three actors in the chain of the deep fake and investigates to what degree the Nigerian law penalizes each actor.

Creators

Creators rank highly across all three criteria of knowledge, intent, and control. They are generally aware of the falsity of the content they produce, may act with deceptive or malicious intent, and exercise direct control over its creation and initial dissemination (Chesney & Citron, 2019). These factors make creators the actors most directly responsible for deepfake-related harm and, therefore, the primary candidates for liability.

In Nigeria, however, the legal protection available in cases involving deepfakes remains largely dependent on the application of existing legal provisions rather than legislation specifically designed to address deepfake creation. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, contains offenses relating to identity theft, impersonation, and cyberstalking that may be relevant where deepfakes are used to facilitate fraud, impersonate individuals, or engage in harassment. The applicability of these provisions nevertheless depends on the specific conduct involved and whether the relevant statutory elements can be established. The Violence Against Persons (Prohibition) Act 2015 (VAPP Act) provides a potential legal basis for addressing certain forms of violence and abuse associated with synthetic intimate imagery. However, its territorial application requires careful qualification. The federal Act was enacted to apply within the Federal Capital Territory (FCT), Abuja, while comparable protection elsewhere depends on the applicable state legislation, including state enactments adopting or adapting the VAPP framework. Consequently, the Act should not be presented as a uniform statutory regime applicable throughout Nigeria. The availability of remedies for victims of deepfake-related abuse must instead be assessed in light of the legislation applicable in the relevant jurisdiction. Furthermore, although existing provisions may address certain forms of abuse, the absence of express references to synthetic intimate imagery leaves questions about the adequacy of existing offenses and remedies in addressing the distinctive characteristics of deepfakes. The Nigeria Data Protection Act 2023 will apply if a person's identity (including their face or voice) is processed without a lawful basis. There is not much else in the Copyright Act 2022 as a person's likeness is not a work. The chief problem is that there are no offenses with names that specifically mention synthetic intimate images or deepfakes, only those that were created earlier apply.

Distributors

Distributors are the most diverse group among the three categories, there are different levels of knowledge, many share fakes thinking that the fake is the real one, humans are not capable of distinguishing them (Köbis et al., 2021), and some are sharing their content with knowledge for the purpose of increasing harm. The spread of intent and control is the same, but control is typically low to medium because a person's control is only over his own share.

There is a mens rea requirement for criminal liability to apply to a Nigerian law, and this is the reason it fits only the knowing distributor, this is proper. One effect of section 39 on expression would be an unjust one, to punish innocent sharers (van der Sloot & Wagensveld, 2021). The problem is proof. It is difficult to prove that a video is false, especially combined with the additional difficulty of compliance with the Conditions in Section 84 of the Evidence Act 2011, which are the same for computer generated evidence. A more realistic path towards a monetary claim is civil claims of defamation or privacy, which require a lower standard of proof of negligence and which can be long and expensive.

Platforms

Platforms have a unique profile, they have low intent to harm, but they have a high extent of knowledge, primarily because they receive notification after they have occurred, and high degree of control over the way in which content is being hosted, ranked, and amplified. Therefore, the control is an ideal point for intervention (Chesney & Citron, 2019).

The NITDA Code of Practice prescribes lots of duties following a notification to a platform and requires a platform to shutter the content and maintain it down. This is a good approach but will react rather than proactively. Like a comparable UK approach, Kira (2024) writes, there is insufficient protection for victims when a video has already been shared, and no labeling or proactive detection provisions within the code for coverage of specific risks associated with the deepfakes phenomenon, including re-uploads.

Prevention Methods

There are three types of answers to the harm caused by deepfakes; technical detection and provenance methods, actual disclosure and takedown obligations, and platform self-regulation. There are definite ethical barriers that each one has.

Technical measures

Generation techniques have developed with detection research. Detection research has been developing as well, though not with the same accuracy. The field is surveyed to identify several dozen methods for detecting deepfakes in a picture or video, with a caveat that when creating a detector using one generation method it does not generalize to newer methods (Masood et al., 2023; Pei et al., 2024). This point has been shown at scale in practice at Meta's own Deepfake Detection Challenge. The best model achieves 82.56% accuracy on their public test set, but they expect the actual "black box" test set to simulate a realistic setting with an accuracy of 65.18%. This serves as a lesson that detection is not enough to serve as a sustainable barrier.

Content provenance is a complementary approach, which is content detection that takes place preemptively. The Coalition for Content Provenance and Authenticity (C2PA) is a free standard supported by Adobe, BBC, Microsoft, Intel, and more that attaches cryptographically signed “Content Credentials” to media at the time of the creation or edit, leaving proof of its source and edit history so that when it is altered, it can be identified rather than require a classifier to do so after the fact. In 2024, major platforms like TikTok, Meta (Facebook, Instagram) and YouTube have started implementing or developing on the standard for AI-generated content. Provenance systems place the responsibility of determining the authenticity of content from "what" onto "how" but require adoption at creation time and have no means of protecting content from outside of the participating tools.

Legal disclosure and takedown duties

Two legal leverage points are reflected through the comparative jurisdictions analyzed earlier. Disclosure, one of the key provisions of Article 50 of the EU AI Act is that deployers must make it clear that the content is artificially generated or manipulated, except in certain narrowly drawn exceptions, like for law-enforcement purposes, or content generated under human control. While the second is Take Down, The legal status of the National Information Technology Development Agency (NITDA) Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries 2022 requires careful examination when assessing intermediary responsibility for deepfake-related harms. The Code expressly identifies section 6 of the National Information Technology Development Agency Act 2007 as its enabling authority and states that it was issued in collaboration with the Nigerian Communications Commission (NCC) and the National Broadcasting Commission (NBC). Section 6 provides the statutory basis for NITDA’s functions concerning the coordination, monitoring, evaluation and regulation of information technology practices, activities and systems in Nigeria. The Code consequently establishes a regulatory framework addressing platform conduct, including complaint-handling procedures, the removal of specified unlawful and non-consensual content, due diligence, risk assessment following notification, and mechanisms for reviewing content-removal decisions (NITDA, 2007; NITDA, 2022).

The US TAKE IT DOWN Act sets a clear 48 hour limit for removal of a defined class of harm (deepfakes of intimate imagery, which must be prohibited at the source and therefore non-consensual). Disclosure and takedown represent two different positions on the harm cycle, disclosure seeks to do something at the point of publishing to stop the deception which may take place. Takedown occurs after the content is already out, and does not replace disclosure.

Platform policy

In addition to fulfilling their legal obligations, the largest platforms implemented their own AI labeling policies in 2023 to 2024. Meta started labeling photo-realistic images created using AI in 2024 for its Facebook, Instagram and Threads platforms, via a mix of a C2PA metadata detection strategy and a programme of voluntary creator labels. In March 2024, YouTube added a similar "altered or synthetic" disclosure requirement for realistic AI content, with enforcement in the beginning of 2025, and updated its privacy rules to permit people to ask for the deletion of AI generated content based on their own likenesses. The content standard C2PA was also implemented by TikTok in the same year, and creators will be required to mark the images that were realistic AI generated. Not enacted as legislation or even a legal requirement binding the users to the terms of the platforms, not the law; they rely on the platforms' ability to detect violations through means other than statute, and user reported violations do not come in at a regular frequency.

DISCUSSION OF FINDINGS

Creations are rated highly not just for knowledge and intent but for control and Nigerian law can easily be reached in respect of what they control. There is legislation impacting Nigeria in relation to both of these, namely, the Cybercrimes Act and the VAPP Act and the NDPA. None of these was written with deepfakes in mind, so they deal with the act indirectly, not to their name. This is the first discovery in this paper, Nigeria has no liability gap, at least at the periphery as creators do not have to fall below the threshold of general purpose offenses, however there is a fit gap in practice, the prosecution must stretch the general purpose offence to a specific harm.

The position is more complex for distributors, as their knowledge and intentions may vary considerably. This variation reflects the different circumstances in which deepfakes are disseminated rather than necessarily indicating a flaw in the liability framework. Some individuals may share fabricated content believing it to be genuine (Köbis et al., 2021; Ahmed, 2021), while others may knowingly circulate content they recognize as false. Accordingly, a uniform liability rule may not adequately account for the differing levels of knowledge and culpability within this group.

Excluding innocent sharers from criminal liability is consistent with the requirement to establish the requisite *mens rea* for a criminal offence. However, this protection may also create an evidentiary difficulty. Individuals who knowingly distribute deepfakes may avoid criminal liability where the prosecution cannot sufficiently prove their knowledge or intention. As discussed in the preceding sections, Nigeria's evidentiary framework may make establishing this mental element particularly challenging. Civil liability may therefore provide victims with an alternative avenue for redress, given the generally lower standard of proof applicable in civil proceedings compared with criminal trials. Nevertheless, civil litigation may be lengthy and costly, potentially limiting victims' ability to obtain effective remedies.

Platforms have a low intent, high control and should be a big point of responsibility under the research framework. Nigeria's NITDA Code is reactive duty and only comes with notice. It is narrower than the UK Online Safety Act 2023, which brings together two distinct duties: a notice and takedown obligation (s.10(3)) with an obligation to take proactive steps to reduce the threat of online harm spreading (s.10(2)). However, Kira (2024) finds the UK's systems and processes" approach to be inadequate for the non-consensual intimate deepfakes in particular as it fails to differentiate synthetic media under its platform rules and provides victims with remedial measures only after the content is already in circulation. The detection technology will not be able to detect harmful content in time (as outlined in the result of the Meta Deepfake Detection Challenge, it is able to reach only an accuracy of 65.18% under realistic conditions). There are, in addition, the requirements for the level of provenance and standards (e.g. C2PA) as a prerequisite for adoption at the point of creation, which is of no help towards harm created outside the standards from which the technology is built.

Overall, the three actor profiles point to a specific solution to Who is liable?. Liability is now strong in principle for the creator, fairly strong in enforcement, whilst it is weak in enforcement for the distributor and absent for the platform so far as Nigeria is concerned, where even a proactive layer is missing. None of these three failures has anything to do with the absence of a missing legal category. Indeed, Nigeria has other sections of the law that would address these failures, such as distributor torts, the duty of platforms to take down creators. The reason is none of these instruments was conceived with the special and low detect-ability characteristics of deepfakes in mind and their need to be distributed quickly and cheaply.

CONCLUSION

This study sought to measure the extent to which Nigerian law addresses the risk and liability of the three actors in the deepfake chain, creator, distributors, and platforms before learning from the comparative data what measures can be taken to fill in the gaps, if any. As demonstrated in the preceding sections, the primary legal gap in Nigeria is not necessarily the absence of applicable legal categories. Rather, the existing framework can address different forms of conduct, creator conduct may be regulated under the Cybercrimes Act, distributor conduct may attract civil liability where knowledge can be established, and platform conduct may be addressed through the notice-and-takedown requirements under the NITDA Code.

RECOMMENDATIONS

The recommendations set out in this section is derived directly from the gaps identified in the preceding sections;

1. Introduce a specific statutory provision addressing deepfakes rather than relying solely on general offenses. A special provision in the Cybercrimes Act establishing an offence relating to deepfakes, following the EU AI Act's definition of deception in Art. 3(60), would fill this gap while not necessitating a new law.
2. Establish proactive platform duties alongside reactive takedown obligations. Concurrently, the NITDA Code's model is restrictive compared to the current framework in the UK which consists of a proactive risk mitigation obligation on operators (under the Online Safety Act 2023, s.10(2)) and a reactive takedown obligation on operators (under the Online Safety Act 2023, s.10(3)). As Nigeria's regulatory capacity has proven to be limited, this could close the gap with the UK model if there were a corresponding obligation placed on the provider, based on risk assessment, and even with a relatively small one.
3. Set a clear deadline for removing the most serious category of harmful content. The NITDA Code restates a point which is that the Code does not have a time limit for deepfake content, unlike the US TAKE IT DOWN Act, which mandates that non-consensual intimate imagery be removed within 48 hours. Nigeria might consider imposing a similar absolute time limit on this more narrow, less contestable class of harm, while imposing a more flexible deadline on the more contestable class of harm like political analysis.
4. Add a satire and parody exception. The NITDA Code does not establish any distinction between "protected satire" and 'falsifying harms'. Art. 50(4) of the EU AI Act does not draw such a distinction, the NITDA Code does not either. Based on the problem of over-censorship, any new deepfakes provision for Nigeria should adopt the EU guideline and ensure a balance between takedown requirements and freedom of expression for the removal of content, namely an ‘evidently artistic, satirical or fictional’ exception that allows for disclosure without necessarily removal.

No component of any of these recommendations fully resolves the free expression/harm dilemma found. The realistic objective is to close the gap relative to the already in place and more developed frameworks of other countries, and not to craft a perfect rule that none of the comparators has yet manifested.

REFERENCES

1. Ahmed, S. (2021). Who inadvertently shares deepfakes? Analyzing the role of political interest, cognitive ability, and social network size. Telematics and Informatics, 57, 101508. https://doi.org/10.1016/j.tele.2020.101508

2. Aylett, M. P., Ching, D., Linehan, C., Murphy, G., Quayle, M., & Twomey, J. (2023). Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. PLOS ONE, 18, 1–22. https://doi.org/10.1371/journal.pone.0291668
3. Alabi, M. (2025). Is AI coming for your face? Premium Times. https://www.premiumtimesng.com/tag/cybercrimes-prohibition
4. Birrer, A., & Just, N. (2025). What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. New Media & Society, 27(12), 6819–6838. https://doi.org/10.1177/14614448241253138
5. Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107, 1753–1820.
6. Coalition for Content Provenance and Authenticity. (n.d.). About C2PA. Retrieved 2026, from https://c2pa.org/about/
7. Constitution of the Federal Republic of Nigeria (1999, as amended).
8. Copyright Act 2022 (Nigeria).
9. Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Nigeria), as amended by the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024.
10. Dan, V. (2025). Deepfakes as a democratic threat: Experimental evidence shows noxious effects that are reducible through journalistic fact checks. The International Journal of Press/Politics. Advance online publication. https://doi.org/10.1177/19401612251317766
11. Ekpang, J. E., Iyorza, S., & Ekpang, P. O. (2023). Social media and artificial intelligence: Perspectives on deepfakes' use in Nigeria's 2023 general elections. KIU Interdisciplinary Journal of Humanities and Social Sciences, 4(2), 109–124. https://doi.org/10.59568/KIJHUS-2023-4-2-08
12. European Union. (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act). Official Journal of the European Union. https://artificialintelligenceact.eu/article/50/
13. Evidence Act 2011 (Nigeria), as amended.
14. Fallis, D. (2021). The epistemic threat of deepfakes. Philosophy & Technology, 34(4), 623–643.
15. Kira, B. (2024, April 30). When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act [Conference presentation]. Sussex AI Seminar, University of Sussex, Brighton, UK. https://www.sussex.ac.uk/broadcast/read/64448
16. Köbis, N. C., Doležalová, B., & Soraperra, I. (2021). Fooled twice: People cannot detect deepfakes but think they can. iScience, 24(11), 103364.
17. Kuźnicka-Błaszkowska, D., & Kostyuk, N. (2025). Emerging need to regulate deepfakes in international law: The Russo–Ukrainian War as an example. Journal of Cybersecurity, 11(1), tyaf008. https://doi.org/10.1093/cybsec/tyaf008
18. Łabuz, M. (2023). Regulating deep fakes in the Artificial Intelligence Act. Applied Cybersecurity & Internet Governance, 2(1). https://doi.org/10.60097/ACIG/162856
19. Łabuz, M., & Nehring, C. (2024). On the way to deep fake democracy? Deep fakes in election campaigns in 2023. European Political Science, 23(4), 454–473. https://doi.org/10.1057/s41304-024-00482-9
20. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. Applied Intelligence, 53(4), 3974–4026. https://doi.org/10.1007/s10489-022-03766-z
21. Meliala, A. P. P. S., & Utari, I. S. (2026). Policy on the formulation of artificial intelligence accountability for the creation and dissemination of deepfake videos from a criminal law perspective in Indonesia. Law Research Review Quarterly, 12(2), 953–981. https://doi.org/10.15294/lrrq.v12i2.44714
22. Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. Journal of Business Research, 154, 113368.
23. National Association of Attorneys General. (2025). Congress's attempt to criminalize nonconsensual intimate imagery: The benefits and potential shortcomings of the TAKE IT DOWN Act. https://www.naag.org/attorney-general-journal/congresss-attempt-to-criminalize-nonconsensual-intimate-imagery-the-benefits-and-potential-shortcomings-of-the-take-it-down-act/
24. National Information Technology Development Agency. (2022). Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries. https://nitda.gov.ng/wp-content/uploads/2022/06/Code-of-Practice.pdf
25. Nigeria Data Protection Act 2023.

26. Nigeria Data Protection Commission. (2026, February 23). Joint statement on AI-generated imagery and the protection of privacy. https://ndpc.gov.ng/joint-statement-on-ai-generated-imagery-and-the-protection-of-privacy-23-february-2026
27. Olisa Agbakoba Legal. (2021, September 25). Deepfakes in Nigeria: Protection and legal framework against deepfake attacks in Nigeria. https://www.mondaq.com/nigeria/security/1114750/deepfakes-in-nigeria-protection-and-legal-framework-against-deepfake-attacks-in-nigeria
28. Online Safety Act 2023 (UK), s.10. https://www.legislation.gov.uk/ukpga/2023/50/section/10
29. Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. Digital Society, 1(2), Article 19. https://doi.org/10.1007/s44206-022-00010-6
30. Pei, G., Zhang, J., Hu, M., Zhang, Z., Wang, C., Wu, Y., Zhai, G., Yang, J., Shen, C., & Tao, D. (2024). Deepfake generation and detection: A benchmark and survey (arXiv:2403.17881). arXiv. https://arxiv.org/abs/2403.17881
31. Rana, M., Nobi, M. N., Murali, B., & Sung, A. H. (2022). Deepfake detection: A systematic literature review. IEEE Access, 10, 25494–25513.
32. Rini, R., & Cohen, L. (2022). Deepfakes, deep harms. Journal of Ethics and Social Philosophy, 22(2), 143–161. https://doi.org/10.26556/jesp.v22i2.1628
33. Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. Computer Law & Security Review, 58, Article 106162. https://doi.org/10.1016/j.clsr.2025.106162
34. TAKE IT DOWN Act, S.146, 119th Cong. (2025). https://www.congress.gov/bill/119th-congress/senate-bill/146
35. van der Sloot, B., Wagensveld, Y., & Koops, B.-J. (2021). Deepfakes: De juridische uitdagingen van een synthetische samenleving (WODC rapport 3137). Tilburg Institute for Law, Technology, and Society.
36. Violence Against Persons (Prohibition) Act 2015 (Nigeria).
37. Vizoso, Á., Vaz-Álvarez, M., & López-García, X. (2021). Fighting deepfakes: Media and Internet giants' converging and diverging strategies against hi-tech misinformation. Media and Communication, 9(1), 291–300. https://doi.org/10.17645/mac.v9i1.3494
38. Whittaker, L., Letheren, K., & Mulcahy, R. (2021). The rise of deepfakes: A conceptual framework and research agenda for marketing. Australasian Marketing Journal, 29(3), 204–214. https://doi.org/10.1177/1839334921999479