

DEEPFAKES, ARTIFICIAL INTELLIGENCE AND NIGERIAN LAW: IS THE LAW READY FOR SYNTHETIC REALITY?

Rapuluchukwu E. Nduka*

Chidimma V. Nduka**

Abstract

Artificial intelligence has quietly closed the gap between imagination and evidence. A video can now show a person saying words they never spoke, endorsing a product they have never seen, or committing an act they never committed. In February 2026, the Nigeria Data Protection Commission joined more than sixty other global data protection authorities in a joint statement warning of the misuse of artificial intelligence systems that generate realistic images and videos of identifiable people without their consent. That warning is the immediate trigger for this article, but the underlying question is older than the technology itself. Can Nigerian law keep pace with synthetic reality? This article interrogates that question across five doctrinal fronts: defamation, privacy and data protection, impersonation, the wider cybercrime regime, and the law of evidence. It argues that Nigeria has assembled a serviceable but incomplete legal patchwork, one built for a world of forged documents and stolen passwords rather than fabricated faces and cloned voices, and it proposes a coordinated legislative and institutional response.

Keywords: Deepfakes; Artificial intelligence; Privacy; Defamation; Cybercrime; Evidence; Nigeria

* Rapuluchukwu Ernest NDUKA LL. D (South Africa), LL.M (Strathclyde), LL. B, BL. Senior Lecturer Dept. of Commercial & Industrial Law, Nnamdi Azikiwe University Awka, Anambra State Nigeria. 08103692233, ra.nduka@unizik.edu.ng.

** Chidimma Victory Nduka LL. B, B.L Senior Magistrate, Anambra State Judiciary, Anambra State Nigeria. 08068397360, chyndukachidiogo@gmail.com.

1.0 INTRODUCTION

In January 2026, a Nigerian businesswoman named Ibukun Awosika found herself contradicting a version of herself that never existed.¹ A video circulating widely online showed her promoting an investment platform. She had said nothing of the sort. A month later, Ngozi Okonjo-Iweala, the Director-General of the World Trade Organization, faced the same ordeal. An AI-generated clip showed her endorsing a scheme she had never heard of.² Both women were, in a strict sense, blameless bystanders to their own image. The words came from a machine. The face, disturbingly, was theirs.

These episodes are not isolated curiosities. They are early signals of a technology that has matured faster than the law meant to restrain it. Deepfakes, a portmanteau of deep learning and fake, use neural networks to synthesise convincing audio, video or images of real people doing or saying things they never did or said.³ What began as an academic curiosity in machine learning laboratories has become a tool available to anyone with a smartphone and a few minutes of patience. The barrier to entry, once measured in years of technical training, is now measured in the time it takes to download an application.

Nigeria has not been spared. Health influencers, actors and business executives have had their likenesses conscripted into schemes they never sanctioned. In one documented instance, a fabricated video used the images of Aproko Doctor, a popular health content creator, and Taiwo Ajai-Lycett, a veteran actor, to promote a purported cure for

¹M Balogun “GUIDE: Scam trends to watch out for in 2026 and how to stay safe online” <GUIDE: Scam trends to watch out for in 2026 and how to stay safe online - Africa Check> accessed 24 July 2026.

²*Ibid.*

³P Osuagwu “Deepfakes in trouble” <<https://www.vanguardngr.com/2026/03/deepfakes-in-trouble/>> accessed 24 July 2026.

hypertension.⁴ The victims range from the famous, whose faces lend credibility to scams, to ordinary citizens, whose images are repurposed for harassment, extortion or humiliation. The harm is not merely reputational. It touches privacy, personal security, financial safety and, in the most serious cases, the integrity of democratic processes.

It was against this backdrop that the Nigeria Data Protection Commission, led by its National Commissioner and Chief Executive Officer, Dr Vincent Olatunji, endorsed a joint statement on AI-generated imagery and the protection of privacy on 23 February 2026.⁵ The statement, coordinated by the International Enforcement Cooperation Working Group of the Global Privacy Assembly and signed by more than sixty data protection authorities worldwide, raised alarm over the use of generative AI to produce non-consensual intimate images, defamatory content and other harmful material. Children and other vulnerable groups were identified as being at particular risk.⁶ The Commission indicated that compliance audit returns filed under the Nigeria Data Protection Act 2023 would now serve as one benchmark for assessing how organisations deploy AI systems that process personal data.⁷

The joint statement did not create new binding rules. It signalled something arguably more important: a coordinated regulatory posture, and an admission that the existing legal terrain is being tested by a technology it was not built to anticipate. This article takes that

⁴*Ibid.*

⁵“Joint Statement on AI-Generated Imagery and the Protection of Privacy” <[2026-02-23-joint-statement-ai-generated-imagery-61-signatories.pdf](#)> accessed 24 July 2026.

⁶R Ibeh “Nigeria joins 60 global regulators to crack down on AI-generated deepfakes” <[https://businessday.ng/technology/article/nigeria-joins-60-global-regulators-to-crack-down-on-ai-generated-deepfakes/](#)> accessed 24 July 2026.

⁷S Akintaro “NDPC joins 60 global DPAs to tackle AI-generated image abuse” <[NDPC joins 60 global DPAs to tackle AI-generated image abuse - Nairametrics](#)> accessed 24 July 2026.

admission as its starting point and asks a direct question. Is Nigerian law ready for synthetic reality?

The inquiry proceeds across five fronts. It begins with the law of defamation, the oldest and most intuitive legal response to a false and damaging statement. It then turns to privacy and data protection, the constitutional and statutory terrain most directly engaged by the unauthorised use of a person's face. From there it examines impersonation and identity theft, offences created with the digital fraudster in mind but increasingly relevant to the deepfake scammer. It considers the broader cybercrime framework within which these offences sit, and the practical difficulties of enforcement. Finally, it confronts the law of evidence. Even where a cause of action exists, a court must still be persuaded that the fabricated video is what the claimant says it is or is not what the defendant says it is. The article closes with reform proposals, informed by the gaps identified across each of these fronts.

2.0 UNDERSTANDING THE TECHNOLOGY

Deepfake technology rests on a family of machine learning methods, most notably generative adversarial networks and, more recently, diffusion models. In simple terms, a generative adversarial network pits two algorithms against each other. One, called the generator, tries to produce a fake image or video frame that looks authentic. The other, called the discriminator, tries to detect the fake. Over many rounds of this contest, the generator improves until its output can fool not only the discriminator but also the human eye. Diffusion models take a different route. They gradually remove digital noise from a random pattern until a coherent image emerges, guided by a text prompt or a reference photograph.

The output of these techniques falls into several rough categories. Face-swap videos superimpose one person's face onto another person's

body. Voice cloning tools recreate a person's speech patterns from a short audio sample, sometimes as brief as a few seconds. Full synthetic video generation now allows an entire scene, background, gestures and lip movements included, to be produced from a single photograph and a script. Still images, meanwhile, can be generated entirely from a text description, or altered so that a real photograph shows a person in a place they never visited.

Each category raises its own legal texture. A face-swapped video used in an intimate or sexualised context implicates privacy and dignity most acutely. A cloned voice used to authorise a bank transfer implicates fraud and computer-related forgery. A synthetic video showing a public figure endorsing a fraudulent investment scheme implicates defamation, fraud and impersonation all at once.⁸ It is this convergence of harms, rather than any single wrong, that makes deepfakes a distinctive legal problem. A single fabricated video can, in principle, support an action in defamation, a complaint under the data protection framework, a criminal charge for impersonation, and a dispute over the admissibility of the very video itself as evidence.

3.0 THE NIGERIAN REGULATORY LANDSCAPE BEFORE AND AFTER FEBRUARY 2026

The February 2026 joint statement did not emerge from a vacuum. It sits within a broader, still developing architecture of AI governance in Nigeria. The Minister of Communications, Innovation and Digital Economy, Dr Bosun Tijani, had earlier led the process that produced Nigeria's National Artificial Intelligence Strategy, finalised in September 2025, setting out the government's ambitions for the responsible development and deployment of AI across the economy.⁹ The Nigerian Bar Association's Section on Legal Practice also issued

⁸P Osuagwu (n 3).

⁹Federal Ministry of Communications, Innovation and Digital Economy, National Artificial Intelligence Strategy (Federal Republic of Nigeria, September 2025).

guidelines on the use of artificial intelligence in legal practice in August 2024, addressing, among other things, the ethical obligations of lawyers who rely on AI tools.¹⁰ Neither instrument, however, speaks directly to deepfakes as a phenomenon of harm to ordinary citizens.

The Commission's own account of its role has since expanded beyond the February statement. At the 2026 Press Week organised by the Federal Capital Territory Council of the Nigeria Union of Journalists, the Commission, represented by its Head of Media Unit, Itunu Dosekun, warned that AI-generated disinformation, targeted political profiling and the misuse of personal data could threaten the credibility of Nigeria's 2027 general election, a poll brought forward to 16 January 2027.¹¹ This warning connects the deepfake problem to a wider concern about electoral integrity. It suggests that the Commission sees itself as having a role in this space, even though the Nigeria Data Protection Act 2023 was not drafted with synthetic media specifically in mind.

A recognised commentary on the Commission's practical reach has observed that the NDPA is fundamentally a data protection statute, calibrated around the relationship between a data subject and a data controller, and that its enforcement architecture was not built for the real-time takedown of viral fraudulent content.¹² As at the time of writing, the Commission had not taken any enforcement action specifically targeting deepfake misuse, notwithstanding its February

¹⁰Nigerian Bar Association, Section on Legal Practice, Guidelines on the Use of Artificial Intelligence in Legal Practice (NBA-SLP, August 2024).

¹¹I Balogun "AI-powered disinformation could threaten Nigeria's 2027 elections, NDPC warns" <[AI-powered disinformation could threaten Nigeria's 2027 elections, NDPC warns - Technology Times | Latest and Breaking Nigeria Tech News](#)> accessed 25 July 2026.

¹²M Alabi "Is AI coming for your face?" <[Is AI coming for your face? | The Cable](#)> accessed 25 July 2026.

2026 endorsement of the joint statement.¹³ This gap between rhetorical concern and operational capacity is a recurring theme of this article. It is visible across each of the doctrinal areas considered below.

4.0 DEFAMATION AND THE SYNTHETIC LIE

Defamation is, historically, Nigeria's first line of response to a false and damaging statement about a person. The tort protects a plaintiff's right to the good name, reputation and standing they enjoy among their fellow citizens.¹⁴ A statement is defamatory where it lowers the claimant in the estimation of right-thinking members of society, exposes them to hatred, contempt or ridicule, causes others to shun or avoid them, or discredits them in their trade, business or profession.¹⁵ The Supreme Court's decision in *Sketch Publishing Co Ltd v Ajagbemokeferi* remains the most frequently cited authority for this formulation in Nigerian jurisprudence, and it has been applied consistently in later cases such as *Guardian Newspapers Ltd v Ajeh*.¹⁶ The English case of *Sim v Stretch* supplies a similar test, and Nigerian courts continue to draw on it.¹⁷

An action in libel, the written or permanent form of defamation, requires a claimant to establish that the words complained of were published, that the publication was to a third party, that the words are defamatory in the sense described above, that they refer to the claimant, and that the defendant was responsible for the publication.¹⁸ Libel is actionable without proof of special damage. Damages are

¹³*Ibid.*

¹⁴*Scott v Sampson* (1882) 8 QBD 491, 503.

¹⁵*Sun Publishing Ltd v Dumba* (2020) 2 NWLR (Pt 1708) 325, 343.

¹⁶*Sketch Publishing Co Ltd v Ajagbemokeferi* (1989) 1 NWLR (Pt 100) 678 (SC); *Guardian Newspapers Ltd v Ajeh* (2011) LPELR-1343 (SC); (2011) 10 NWLR (Pt 1256) 574.

¹⁷*Sim v Stretch* (1936) 2 All ER 1237.

¹⁸*Guardian Newspapers Ltd v Ajeh* (n 16).

presumed to flow naturally from the publication once defamation is established.¹⁹

At first glance, a deepfake video appears to fit neatly within this framework. It is published, in the sense that it is broadcast or shared to third parties. It plainly refers to the claimant, since the entire point of the exercise is to use their recognisable face and voice. It is capable of being defamatory, particularly where it shows the claimant endorsing a fraudulent scheme, making an offensive remark, or engaging in conduct that would embarrass or discredit them. On these three elements, the deepfake victim is arguably in a stronger position than the traditional libel claimant. The identification requirement, often a point of dispute in ordinary defamation suits, is rarely contestable when the claimant's own face has been superimposed onto the offending content.

The real difficulty lies elsewhere, in the requirement that the claimant establish who is responsible for the publication. Traditional defamation defendants are usually easy to identify, a newspaper, a broadcaster, an individual with a known social media account. Deepfake content, by contrast, often originates from anonymous or pseudonymous accounts, is hosted on servers outside Nigeria, and spreads through resharing long before the original poster can be traced. A claimant may succeed in establishing every substantive element of the tort and still find themselves without a defendant worth suing.

A further complication concerns the defences ordinarily available in defamation actions. Justification, or truth, is unavailable to a deepfake publisher because the content is by definition false. Fair comment likewise fails, since the defence protects honestly held opinion on a matter of public interest rather than a fabricated depiction of fact. In

¹⁹Chief Tony Okoroji v Onyeka Onwenu (2016) LCN/9036 (CA).

principle, deepfake defamation should be easier to win on the merits than conventional defamation, precisely because the usual defences do not apply. The practical bottleneck is not the substantive law of defamation. It is the identification of a solvent, traceable defendant, and the platform-level question of who bears responsibility when the original poster cannot be found.

There is also a criminal dimension. Nigeria's Criminal Code and Penal Code both contain offences of criminal defamation, sitting alongside the civil tort.²⁰ These provisions have historically been used sparingly and have attracted criticism for their potential misuse against journalists and government critics. Whether they would, or should, be deployed against deepfake creators is a separate policy question. Their existence means that a deepfake victim theoretically has both civil and criminal avenues, subject to the same difficulty of identifying the perpetrator.

5.0 PRIVACY, DATA PROTECTION AND THE RIGHT TO ONE'S LIKENESS

If defamation protects reputation, privacy protects something more personal, the right to control what is done with one's own image, voice and identity. Section 37 of the Constitution of the Federal Republic of Nigeria 1999, as amended, guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.²¹ The provision does not mention biometric data or artificial intelligence, for the obvious reason that it was drafted decades before either was a live legal concern. Nigerian courts have nonetheless shown a willingness to read the provision generously. The Court of Appeal held in *Digital Rights Lawyers Initiative v National*

²⁰Criminal Code Act, Cap C38, Laws of the Federation of Nigeria 2004; Penal Code (Northern States) Federal Provisions Act, Cap P3, Laws of the Federation of Nigeria 2004.

²¹Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

Identification Management Commission that the constitutional right to privacy extends to data protection, since the two are, by definition, closely related.²²

The Nigeria Data Protection Act 2023 gives this constitutional guarantee statutory texture. The Act defines biometric data as a category of sensitive personal data. Processing of sensitive personal data requires a lawful basis, ordinarily the data subject's explicit consent.²³ A commentary on the Act's practical reach has argued that the unauthorised use of a person's face to generate synthetic content is, in substance, a form of biometric data processing without consent, and that a credible argument exists for treating this as a breach of the NDPA's core prohibitions.²⁴ The difficulty, as the same commentary observes, is institutional rather than doctrinal. The Commission's enforcement machinery is built around compliance audits, sectoral guidance and the regulation of data controllers with an ongoing relationship with the Commission. It is not designed for the urgent, borderless problem of a viral deepfake circulating on platforms with no Nigerian office and no obligation to respond to a Nigerian regulator's request within hours rather than weeks.²⁵

A further gap concerns what common law jurisdictions sometimes call the right of publicity, or the tort of appropriation of name or likeness. This is a well-developed area of law in some jurisdictions, protecting both the dignitary interest in being left alone and the commercial

²²Digital Rights Lawyers Initiative v National Identification Management Commission (2021) LPELR-55623(CA). See also, S Ngwu "Friction of Rights: Copyrights in a Photograph, Image Rights and Data Protection Rights of the Photographed" <[Friction Of Rights: Copyrights In A Photograph, Image Rights And Data Protection Rights Of The Photographed – Balancing The Rights - Privacy Protection - Nigeria](#)> accessed 25 July 2026.

²³Nigeria Data Protection Act 2023, ss 24 to 26 and s 30.

²⁴M Alabi (n 12).

²⁵*Ibid.*

interest in controlling the exploitation of one's identity.²⁶ Nigeria has no comprehensive national legislation of this kind. The most direct statutory equivalent exists only in Lagos State, where the Law Reform (Torts) Law makes it actionable to use the name or likeness of another in a manner that suggests an intention to appropriate that identity or an association with it without consent.²⁷ This is a meaningful protection, but its territorial limits are significant. A deepfake victim resident in Kano, Enugu, or Port Harcourt has no equivalent statutory cause of action and would need to rely on the less settled route of a general constitutional privacy claim or on the Nigeria Data Protection Act, neither of which was designed with commercial image misappropriation specifically in view.

The cumulative picture is one of partial, geographically uneven and doctrinally scattered protection. A claimant's remedy for the same underlying harm, the unauthorised synthetic use of their face, may depend on which state they live in, whether they can characterise the harm as a privacy violation, a data protection breach, or a common law tort, and whether the defendant is identifiable and within the jurisdiction. This is not a satisfactory state of affairs for a harm that, as the February 2026 joint statement makes clear, regulators around the world now regard as a matter of pressing concern.

6.0 IMPERSONATION, IDENTITY THEFT AND THE CYBERCRIME FRAMEWORK

Nigeria's principal cybercrime statute, the Cyber Crimes (Prohibition, Prevention, etc) Act 2015, creates a specific offence of identity theft and impersonation.²⁸ The provision was amended in 2024 to widen its

²⁶Restatement (Second) of Torts (American Law Institute) s 652C, discussing the tort of appropriation of name or likeness in comparative common law terms.

²⁷Law Reform (Torts) Law, Laws of Lagos State 2015, Cap L82; See also, A Etete "Nigeria Media Law Guide" <[Nigeria - Carter-Ruck](#)> accessed 26 July 2026.

²⁸Cyber Crimes (Prohibition, Prevention, etc) Act 2015, s 22.

reach. Under the original Act, only persons connected with financial institutions could be held liable for this offence. The amendment extended liability to persons engaged in the services of public and private organisations generally, a change that brings a wider range of impersonation conduct within the section's scope.²⁹ The Act also creates an offence of cyberstalking, targeting conduct that causes annoyance, alarm or distress by means of a computer system or network.³⁰ This provision has obvious relevance to the harassment dimension of non-consensual deepfake content.

Applied to the deepfake context, the impersonation offence offers a plausible criminal route against a person who fabricates and disseminates AI-generated content bearing another person's likeness for fraudulent purposes, such as the fake investment endorsements that circulated using the images of Ibukun Awosika and Ngozi Okonjo-Iweala.³¹ The conduct fits the ordinary meaning of impersonation. The difficulty, once again, is not the availability of the offence but the practicalities of enforcement. The Act's investigative and prosecutorial machinery depends on identifying a perpetrator, securing cooperation from platforms that may be based outside Nigeria, and establishing a chain of evidence linking a specific individual to the creation and publication of the content. Cross-border evidence gathering under the Act's international cooperation provisions is possible in principle, but it is slow, and slow is precisely what a viral deepfake does not allow for.³²

²⁹Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act 2024, s 22; "Cybercrimes Amendment Act Exposes Lapses in Legislative Process" <[Cybercrimes Amendment Act Exposes Lapses in Legislative Process – PLAC Legist](#)> accessed 26 July 2026.

³⁰Cyber Crimes (Prohibition, Prevention, etc) Act 2015, s 24.

³¹M Balogun (n 1).

³²Cyber Crimes (Prohibition, Prevention, etc) Act 2015, Part VII.

A related commentary on this problem has argued for a distinct, third layer of regulation: a platform accountability framework, whether administered by the Commission, the Nigerian Communications Commission, or a joint instrument between the two, that would impose defined takedown obligations on social media platforms hosting deepfake fraud content, with clear response timelines and consequences for non-compliance.³³ The argument draws on the observed pattern that once a fabricated video is flagged on one platform, it frequently continues to circulate on others for days, as happened with the Okonjo-Iweala deepfake, which she flagged on one platform while it continued to spread on several others.³⁴ Platforms, on this view, are not neutral conduits. They are part of the infrastructure through which the harm is distributed, and the law arguably ought to treat them accordingly.

The broader cybercrime framework also contains offences of computer-related forgery and the use of fraudulent devices, both of which may apply where a deepfake is used as a step in a wider fraud, such as voice cloning used to authorise a fraudulent bank transfer.³⁵ These provisions were drafted with conventional digital fraud in mind, forged documents, hacked accounts and cloned payment cards, but their language is broad enough to accommodate AI-generated fabrication as a species of the same underlying wrong. What Nigeria currently lacks is any offence, or civil wrong, drafted with the specific vocabulary of synthetic media, one that would name deepfakes as such and calibrate penalties, defences and takedown obligations to the particular way that this technology causes harm.

³³M Alabi (n 12).

³⁴*Ibid.*

³⁵Cyber Crimes (Prohibition, Prevention, etc) Act 2015, ss 13 to 14.

7.0 EVIDENTIAL CHALLENGES: PROVING AND DISPROVING SYNTHETIC MEDIA

Even where a clear cause of action exists, whether in defamation, privacy, data protection or cybercrime, a claimant or prosecutor must still persuade a court that a piece of electronic content is what they say it is. This is where the law of evidence enters, and where deepfakes pose perhaps their most conceptually difficult problem.

Section 84 of the Evidence Act 2011 governs the admissibility of a statement contained in a document produced by a computer.³⁶ The provision permits such a statement to be admitted as evidence of any fact of which direct oral evidence would be admissible, provided the conditions in section 84(2) are satisfied, generally relating to the regularity of the computer's use and production of the document.³⁷ Section 84(4) further requires that a certificate be produced, identifying the document and describing the manner of its production, in order to authenticate the statement.³⁸ The Supreme Court considered these requirements in *Kubor v Dickson*, one of the leading Nigerian authorities on the admissibility of electronic evidence.³⁹ The Court of Appeal, in *Stanbic IBTC Bank v LongTerm Global Capital Ltd*, held that a party who does not possess the device from which a document was produced cannot be compelled to tender a section 84(4) certificate to authenticate it, a decision that narrowed the provision's practical application.⁴⁰

These provisions were designed to solve a specific problem, distinguishing a genuine computer-generated record from an

³⁶Evidence Act 2011, s 84.

³⁷*Ibid*, s 84(2).

³⁸*Ibid*, s 84(4).

³⁹*Kubor v Dickson* (2013) 4 NWLR (Pt 1345) 534 (SC).

⁴⁰*Stanbic IBTC Bank v LongTerm Global Capital Ltd & Ors* (2021) LPELR-55610 (CA).

inadmissible piece of hearsay, and guarding against the alteration of electronic documents after the fact. Deepfakes invert this problem in an important respect. Section 84 is concerned with whether a document was properly produced and has not been tampered with since. It says nothing about whether the content the document records is itself an authentic depiction of an event that occurred. A fabricated video can, in principle, satisfy every formal requirement of section 84. It can be regularly produced, properly stored, and accompanied by a compliant certificate, while depicting an event that never happened at all. The certificate authenticates the file. It cannot authenticate reality.

This is sometimes called, in the wider literature on synthetic media, the liar's dividend, the phenomenon whereby the mere existence of deepfake technology makes it easier for a person responsible for genuine, damaging footage to claim that the footage is fabricated.⁴¹ A litigant confronted with authentic video evidence of their own wrongdoing may now plausibly, if falsely, allege that the video is an AI fabrication, forcing the opposing party to undertake forensic authentication that the Evidence Act does not currently require in explicit terms. Nigerian courts have limited experience with this problem. As one commentary notes, there remains a scarcity of reported Nigerian judicial authority specifically addressing the admissibility of electronic evidence, a gap that has led courts to draw on English and Indian decisions for guidance.⁴²

Practically, this means that Nigerian courts currently have no settled protocol for forensic deepfake detection, no accredited body of expert witnesses on synthetic media analysis, and no statutory presumption

⁴¹See generally the discussion of the evidentiary effects of synthetic media in M Alabi (n 12).

⁴² C Unini "Certificate of Authentication in Admissibility of Electronic Evidence" <<https://thenigerialawyer.com/certificate-of-authentication-in-admissibility-of-electronic-evidence/>> accessed 26 July 2026.

allocating the burden of proving or disproving authenticity once a party raises a credible challenge. The Evidence Act's framework, built in 2011 around the question of whether a computer produced a document reliably, does not contemplate the question that deepfakes now force upon every court, whether the reality depicted in that document ever existed at all. Until this gap is addressed, either through judicial practice directions, forensic accreditation standards, or legislative amendment, litigants on both sides of a deepfake dispute face genuine uncertainty about how a Nigerian court will resolve a contested authenticity claim.

8.0 TOWARDS A NIGERIAN RESPONSE

The preceding analysis suggests that Nigeria is not without legal tools to respond to deepfakes. It is, however, working with tools forged for different problems: reputational harm from a printed word, data misuse within an ongoing controller relationship, digital fraud through stolen credentials, and electronic records whose authenticity was never in doubt as to the underlying event, only as to the fidelity of the copy. A coordinated response might usefully proceed along several lines.

First, Nigeria should consider a dedicated statutory provision addressing synthetic media, whether as an amendment to the Cybercrimes Act or as free-standing legislation. Such a provision could define deepfakes with appropriate precision, distinguish between categories of harm, non-consensual intimate content, fraudulent commercial use, political disinformation, and satire or parody, and calibrate criminal and civil consequences accordingly. The distinction matters. A blanket prohibition risks capturing legitimate creative and journalistic uses of synthetic media alongside genuinely harmful ones.

Second, the patchwork nature of image rights protection deserves legislative attention. A national statute recognising a right against the

unauthorised commercial or reputationally damaging use of a person's name, image or voice would remove the present anomaly whereby a Lagos resident enjoys a statutory cause of action unavailable to a similarly situated claimant elsewhere in the country.

Third, the Commission's enforcement architecture requires a rapid-response capacity distinct from its existing compliance audit mechanism. Compliance audits are useful for assessing how organisations process personal data over time. They are of limited use against an anonymous individual who posts a fabricated video and disappears. A statutory takedown framework, whether administered by the Commission alone or jointly with the Nigerian Communications Commission, imposing defined response timelines on platforms operating in Nigeria, would close a gap that current mechanisms leave open.

Fourth, the judiciary and the wider legal profession require capacity building on the forensic dimension of synthetic media. Judicial training on the technical markers of AI-generated content, together with the accreditation of forensic experts capable of testifying credibly on authenticity questions, would reduce the present uncertainty surrounding contested electronic evidence. The Evidence Act itself may need amendment to place an explicit burden on a party who raises a deepfake challenge to a piece of electronic evidence, so that a bare assertion of fabrication cannot, by itself, defeat evidence that would otherwise satisfy section 84.

Fifth, given the transnational nature of the harm, illustrated vividly by the fact that a single fabricated video can use the likeness of a Nigerian public figure, be hosted on a server outside the country, and circulate to a global audience within hours, Nigeria's continued participation in international cooperative frameworks, of the kind reflected in the

February 2026 joint statement, is not merely diplomatic courtesy. It is a practical necessity. No single national regulator can, acting alone, keep pace with content that respects no border.

9.0 CONCLUSION

The question posed at the outset of this article, whether Nigerian law is ready for synthetic reality, does not admit of a simple yes or no answer. Nigeria has a functioning law of defamation, a constitutional and statutory privacy framework, a cybercrime statute addressing impersonation, and an evidence law that, however imperfectly, accommodates electronic material. Each of these instruments offers a partial answer to the deepfake problem. None was designed for it.

The February 2026 joint statement endorsed by the Nigeria Data Protection Commission is best understood not as a solution but as an acknowledgment, a recognition by Nigeria's own privacy regulator that the existing framework is being tested by a technology that moves faster than legislative process typically allows. The gap between that acknowledgment and a coordinated legislative response remains to be closed. Until it is, victims of deepfakes in Nigeria will continue to rely on a legal patchwork assembled for a different and, in retrospect, simpler age, one in which a lie could be told about a person, but not yet convincingly shown.