International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 22-06-2026, Accepted: 22-07-2026, Published: 06-08-2026
Volume 12, Issue 3, 2026, Page No. 218-227

Deepfake technology regulation: Evaluation of global approaches and Nigerian criminal law frameworks for legal reform

Onyedikachi Chiagoziem Moore[1], Mary Udofia[2], Nwaimo Chidiebere Kingsley[1]
[1] Lecturer, Law Unit, Department of Social Sciences, Federal Polytechnic, Nekede, Owerri, Imo State, Nigeria
[2] Senior Lecturer, Faculty of Law, University of Uyo, Uyo, Akwa Ibom State, Nigeria

Abstract
This study evaluated the regulation of deepfake technology in Nigeria, with particular emphasis on the criminal law challenges associated with artificial intelligence-generated synthetic media and approaches for legal reform. The study explored the development and applications of deepfake technology such as its beneficial uses in entertainment, education, healthcare and communication, while focusing on its misuse in fraud, identity impersonation, non-consensual sexual content, misinformation and manipulation of digital evidence. The research adopted doctrinal methodology which involved the analysis of Nigerian criminal law frameworks, relevant judicial decisions, statutory provisions and comparative regulatory approaches from the European Union, United States, China and United Kingdom. The study finds that existing Nigerian legal instruments; the Criminal Code Act, Penal Code Act and Cybercrimes (Prohibition, Prevention, etc.) Act 2015, provide limited legal responses to some deepfake-related harms but fail to expressly regulate the creation, distribution and malicious use of synthetic media. The findings revealed significant challenges relating to criminal attribution, proof of intent, and authentication of AI-generated evidence, anonymous online actors and cross-border enforcement. Comparative analysis showed that effective deepfake regulation requires specific criminal offences, transparency obligations, technology provider responsibilities, and reliable evidence verification mechanisms and enhanced digital forensic capacity. The study recommended the enactment of deepfake-specific legislation, amendment of existing cybercrime laws and strengthening of institutional capacity for investigation and enforcement.

Keywords: Deepfake technology, Artificial intelligence, Nigeria, criminal law, digital evidence

Introduction

Artificial Intelligence (AI) has evolved from a field of computer science focused on reproducing human cognitive functions into a technology capable of performing activities involving reasoning, learning, perception and decision-making. Russell and Norvig (2016) [57] explained AI through four approaches: machines that think like humans, machines that think rationally, machines that act like humans and machines that act rationally. These approaches showed attempts to develop computational systems capable of carrying out tasks traditionally associated with human judgment (Kertysova, 2018) [31]. AI applications now exist in healthcare, education, finance, security, entertainment and legal practice (Miotti & Wasil, 2024) [40]. In legal services, AI tools are used for document review, legal research, predictive analysis and examination of large volumes of information (Mkpo, 2025) [41]. While these applications improve professional efficiency, they also raise legal questions concerning authenticity, responsibility and the reliability of digitally produced materials.

Generative artificial intelligence refers to systems that create new content such as text, images, audio and video, through patterns derived from extensive datasets (NVIDIA, 2024) [27]. Advances in machine learning, neural networks, Generative Adversarial Networks (GANs) and diffusion models have enabled AI systems to generate realistic synthetic materials (Olasiyan & Olasiyan, 2026) [51]. These developments have produced beneficial applications in fields such as medical research, education, entertainment and cybersecurity. Synthetic datasets, for example, allow researchers and organisations to develop analytical systems without exposing confidential information. Healthcare institutions use artificial datasets for research purposes, while financial organisations employ generated data for system testing and fraud detection (Olasiyan & Olasiyan, 2026) [51]. The same capabilities, however, have created opportunities for identity manipulation, fabricated recordings and artificial representations of real individuals. The capacity of AI systems to reproduce human appearance, voice and behaviour has challenged traditional assumptions about digital authenticity. Courts and investigative bodies have historically relied on photographs, audio recordings, videos and other digital materials as representations of actual events (Oboh, 2025) [47].

AI-generated evidence and synthetic media create difficulties because such materials present false events with realistic accuracy (Mkpo, 2025). Von Eschenbach (2021) [41, 68] identified the "black box" nature of some AI systems, where the processes producing particular outputs were not easily examined or verified. This issue created concerns regarding accountability, reliability and the admissibility of AI-generated materials in judicial proceedings. Deepfake technology represents one of the most disputed applications of generative AI. Deepfakes are manipulated or artificially generated images, videos and audio recordings created through machine learning methods that imitate real individuals and events (Ajder *et al*., 2019) [2]. The technology relies heavily on deep learning techniques, especially GANs, which enable systems to analyse existing data and produce realistic synthetic content (Tolosana *et al*., 2020) [65]. The term "deepfake" gained public attention in 2017 after a Reddit user circulated manipulated pornographic videos that placed the faces of female celebrities onto the bodies of adult performers (Nnamdi,

Oniyinde & Abegunde, 2023) [44]. Although early deepfake production required advanced technical knowledge, the availability of accessible applications has reduced the expertise required for creation. Individuals with limited technical skills can now generate convincing synthetic media through publicly available tools (Nnamdi *et al*., 2023) [44].

Deepfake technology has legitimate uses in film production, advertising, education and accessibility services (Okeke *et al*., 2024) [49]. Filmmakers have used synthetic media to modify scenes, recreate historical personalities and reduce production expenses (Alanazi, Asif & Moulitsas, 2024) [3]. The misuse of the technology has, however, produced serious legal concerns. One major area of abuse involves non-consensual sexual content. Karasavva and Noorbhai (2021) [30] classify deepfake pornography as image-based sexual abuse because artificial intelligence is used to create sexual representations without consent. Deepfakes have also been applied in financial crimes and impersonation schemes. Kshetri (2023) [35] reported a case involving approximately $35 million in losses after criminals used synthetic technology to imitate a company executive. AI-generated voices and images can exploit trust-based verification methods by allowing offenders to impersonate legitimate persons (Bourgault, 2025) [5]. The increased accessibility of deepfake tools has changed the nature of digital fraud by enabling individuals to create convincing false evidence, impersonate others and manipulate public perception.

The criminal justice system faces particular challenges from deepfake technology because evidence evaluation depends heavily on determining whether digital materials accurately represent real events. Deepfakes be used to fabricate evidence, create false alibis, manipulate witness statements, or undermine genuine recordings. Nnamdi *et al*. (2023) [44] argue that synthetic videos enable individuals to present fabricated images indicating their presence or absence at particular locations. This creates difficulties concerning authentication, evidential weight and judicial decision-making. A related concern is the "liar dividend," which occurs when individuals reject genuine evidence by falsely claiming that it has been artificially generated (Chesney & Citron, 2019) [8]. As awareness of deepfake technology increases, accused persons, political actors and organisations attempt to create doubt about authentic recordings. Carpenter (2024) [7] explains that the danger extends beyond fabricated materials because false claims of manipulation weaken confidence in genuine evidence.

Deepfakes also create risks for public trust, political communication and democratic processes as manipulated speeches, fabricated videos and false announcements influence public opinion, damage reputations and increase social tensions. Meskys *et al*. (2020) [39] identify the potential use of deepfakes in elections, misinformation campaigns and attacks on public institutions. Pawelec (2022) [54] further argues that synthetic media contribute to misinformation, hate speech and declining confidence in information sources. Repeated exposure to manipulated content create uncertainty regarding the authenticity of digital information (Alanazi *et al*., 2024) [3]. Nigeria faces similar concerns due to the increasing role of digital platforms in political communication and public interaction. The expansion of internet access and social media participation has created conditions where manipulated content circulate before verification (Sekoni-Dairo, 2026)[61]. Nigerian legal framework for cyber-related offences is mainly contained in the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 [11], which criminalises offences including identity theft, cyberstalking, electronic fraud and unauthorised access to computer systems (FRN, 2015). The legislation, enacted before the widespread adoption of generative AI, does not expressly regulate deepfake creation, distribution, or misuse.

Certain existing laws provide limited remedies for deepfake-related harm such as activities involving impersonation, fraud, or unlawful processing of personal information which fall under provisions of the Cybercrimes Act and the Nigeria Data Protection Act 2023 (Mkpo, 2025) [21, 47]. Sections 34 and 37 of the Constitution of the Federal Republic of Nigeria 1999 [18] (as amended) recognise rights relating to human dignity and privacy. However, these constitutional protections were developed before AI-enabled identity manipulation became possible. Eigbedion (2020) [15] argues that Nigerian law does not specifically recognise deepfakes, although existing legal principles address related offences such as defamation, identity fraud and privacy violations. Enforcement difficulties are increased by the cross-border nature of digital platforms and the possibility that offenders operate outside Nigerian jurisdiction (Olasiyan & Olasiyan, 2026) [51]. Nigerian response to deepfake-related offences is also affected by limitations in cybersecurity infrastructure, forensic resources and technical capacity. Ogana (2017) [48] identifies weaknesses in cybersecurity systems, forensic capability, database management and public awareness as factors affecting cybercrime control. Fehintola (2023) [21] notes that enforcement agencies face difficulties arising from limited expertise and investigative resources. These challenges demonstrate the need for legal rules capable of addressing deepfake creation, distribution, liability and evidential assessment. This study therefore examines the regulation of deepfake technology under Nigerian criminal law by evaluating existing legal provisions, identifying areas requiring reform and considering approaches capable of addressing emerging offences associated with synthetic media.

Overview of Deepfake Technology

Deepfake technology refers to artificial intelligence-based techniques used to create or modify digital materials such as images, videos and audio recordings, in ways that present fabricated representations of persons, events, or communications as authentic (Tolosana *et al*., 2020) [65]. The term "deepfake" combines "deep learning" and "fake," reflecting the use of deep neural networks to analyse existing data and generate synthetic media (Westerlund, 2019; Tolosana *et al*., 2020) [65, 70]. Unlike traditional digital editing, which depends largely on manual alteration, deepfake systems use machine learning models capable of identifying and reproducing patterns relating to human faces, voices, expressions and movements (Chesney & Citron, 2019) [8]. The development of deepfake technology follows earlier forms of image and video manipulation. Digital alteration of photographs existed before AI-generated synthetic media became available, with historical examples showing the modification of images for political and social purposes (Blakemore, 2020) [4]. Artificial intelligence changed the nature of this practice by enabling

automated creation of realistic audiovisual materials without depending entirely on human editing skills.

Public awareness of deepfakes increased in 2017 when a Reddit user identified as "deepfakes" published manipulated videos involving the replacement of celebrities' faces onto explicit content (Meskys *et al*., 2020; Sample, 2020) [39, 60]. Early deepfake production required significant technical knowledge and computing resources. The introduction of accessible applications such as FakeApp in 2018 [58] reduced these barriers and allowed more users to create face-swapping content (Meskys *et al*., 2020) [39]. Since then, deepfake methods have developed beyond basic face replacement into systems capable of voice cloning, synthetic identity creation, facial expression transfer and realistic video generation from limited source materials (Tolosana *et al*., 2020) [65]. Modern deepfake production depends on advances in artificial intelligence, computer vision, neural networks and generative models. Earlier research contributed to these developments such as Face2Face technology created by Thies *et al*. in 2016, which enabled one-person facial movements to control another person facial expressions in video recordings (Meskys *et al*., 2020) [39]. Deepfake systems now employ machine learning techniques capable of analysing images, video frames and audio samples to reproduce characteristics associated with particular individuals (Westerlund, 2019) [70]. These developments have produced legitimate applications while creating opportunities for deception, fraud, harassment, political manipulation and reputation damage.

There is no single definition of deepfake technology. Chesney and Citron (2019) [8] describe deepfakes as hyper-realistic digital images, videos and audio materials manipulated to depict individuals performing actions or making statements that never occurred. Westerlund (2019) [70] defines deepfakes as AI-generated videos that reproduce facial expressions, mannerisms, voices and speech patterns through neural networks. The European Union Artificial Intelligence Act 2024 [49] recognises deepfake content as AI-generated or manipulated image, audio, or video material that resembles existing persons, objects, places, entities, or events and appear authentic to viewers (European Union Artificial Intelligence Act, 2024) [49]. For legal purposes, deepfakes be understood as artificially generated digital media created through deep learning techniques that present false representations in a form capable of misleading viewers (Okoyenta, 2025) [50]. Deepfake technology is closely associated with artificial intelligence, machine learning and deep learning. Artificial intelligence enables computer systems to perform tasks involving recognition, decision-making and content generation.

Machine learning allows systems to identify patterns from data through training processes, while deep learning uses artificial neural networks containing multiple layers to analyse complex information (Kertysova, 2018) [31]. Deepfake creation depends on deep learning because neural networks can process large volumes of facial images, voice samples and behavioural patterns to reproduce human characteristics (Westerlund, 2019) [70]. Convolutional neural networks assist with facial recognition and image processing, while natural language processing techniques support synthetic speech and text generation (Heidari *et al*., 2023) [28]. Generative Adversarial Networks (GANs) represent one of the major technologies used in deepfake production. GANs consist of two neural networks: a generator and a discriminator. The generator creates synthetic content, while the discriminator evaluates whether the output resembles genuine material (Tolosana *et al*., 2020) [65]. Through repeated interaction, the generator improves its ability to produce realistic images, videos and audio recordings (Meskys *et al*., 2020) [39]. Deepfake systems also rely on autoencoders, which compress and reconstruct information to enable the transfer of facial features, expressions and identity characteristics between individuals (Meskys *et al*., 2020) [39].

Deepfakes exist in different forms depending on the type of manipulation involved. Tolosana *et al*. (2020) [65] identify four categories: whole face synthesis, identity swap, attribute manipulation and expression transfer. Whole face synthesis creates artificial faces of persons who do not exist. Identity swap replaces one individual facial identity with another, while attribute manipulation changes features such as age, appearance, or expression. Expression transfer allows the movements of one person to control another person facial behaviour. Deepfakes also appear as synthetic audio, video, images and text. Voice cloning technology can reproduce speech patterns, while natural language processing systems can generate written content capable of supporting misinformation activities (Sullivan-Paul, 2023) [63]. The technology has produced beneficial applications in entertainment, education, healthcare and communication. Film producers use deepfake methods to modify scenes, recreate historical figures and reduce production costs (Eigbedion, 2020) [15]. Synthetic voices have assisted individuals who have lost speech abilities because of illness, while educational campaigns have used artificial voice and facial technologies to communicate information in multiple languages. A malaria awareness campaign involving David Beckham demonstrated how synthetic media could support multilingual public communication (Eigbedion, 2020) [15].

Healthcare researchers have also examined synthetic data generation as a method of protecting privacy while supporting medical research (Olasiyan & Olasiyan, 2026) [51]. Despite these applications, deepfake technology has created serious criminal law concerns. Non-consensual sexual deepfakes represent a major category of abuse because fabricated sexual images and videos be produced and distributed without consent, causing privacy violations, reputational injury and psychological harm (Meskys *et al*., 2020; Bourgault, 2025) [5, 39]. Deepfakes have also been used for political manipulation through fabricated speeches, false statements and misleading recordings attributed to public figures (Meskys et al., 2020) [39]. Such materials create difficulties for democratic processes and public confidence in digital evidence. Financial crimes involving deepfakes have increased concerns regarding identity verification and fraud prevention.

Criminal actors have used AI-generated voices and synthetic identities to impersonate executives and obtain financial benefits. Synthetic identity fraud combines genuine personal information with fabricated biometric features to create false identities capable of deceiving automated verification systems (Ryman-Tubb, Krause & Garn, 2018) [58]. The use of deepfake-generated faces, voices and documents creates additional challenges for financial institutions and law enforcement agencies because fabricated identities appear consistent with legitimate records (Kietzmann *et al*., 2020) [33]. The dual nature of deepfake technology, offering both beneficial applications and opportunities for criminal

exploitation, has made regulation a significant issue for contemporary legal systems.

The Nigerian Criminal Law Framework on Deepfake Technology

1. The Criminal Code Act

The Criminal Code Act remains one of the legal instruments capable of addressing certain harmful applications of deepfake technology despite predating the emergence of artificial intelligence-generated media. The Act does not contain provisions that expressly mention deepfakes, synthetic media, or artificial intelligence manipulation. However, some of its provisions relating to forgery, false pretences, impersonation and fraudulent conduct apply where deepfake content is used to deceive victims, obtain unlawful benefits, or damage the reputation of another person (Obalola & Omotayo, 2021; Eguridu *et al*., 2024) [14, 30]. The application of traditional criminal offences to deepfake-related conduct depends on establishing the required elements of criminal responsibility under Nigerian law. Criminal liability requires both the commission of a prohibited act and the existence of a guilty state of mind. This principle, expressed through the maxim *actus non facit reum nisi mens sit rea*, remains a recognised foundation of Nigerian criminal jurisprudence. A person who creates or distributes a manipulated video, image, or audio recording with knowledge of its falsity and an intention to cause harm fall within existing criminal provisions where the facts satisfy the requirements of the offence (Eguridu *et al*., 2024)[14]. The Supreme Court of Nigeria has affirmed that criminal responsibility requires proof of the essential ingredients of an offence and that the prosecution must establish both the act constituting the offence and the mental element required by law. In *Adebayo v State [2014] 12 NWLR (Pt. 1421) 613*, the Court held that the prosecution bears the burden of proving the ingredients of a criminal offence beyond reasonable doubt before conviction can follow. This principle applies to deepfake-related prosecutions because the prosecution would be required to establish that the accused person created, distributed, or used manipulated digital content with the necessary criminal intention.

Forgery provisions under sections 365 and 366 of the Criminal Code Act address the falsification of documents and representations. Although these provisions were developed before electronic communication became widespread, their application has extended to digital environments where false electronic documents, signatures, approvals and records are created or presented as genuine (Obalola & Omotayo, 2021). Nigerian courts have recognised that forgery involves the creation of a false document or representation with fraudulent intent. In *R v Ogbuewu [1949] 12 WACA 483*, the court considered the nature of forgery and the requirement that the false document must be created in circumstances capable of deceiving another person. The reasoning in the case supports the application of forgery principles to modern digital environments where fabricated materials are presented as authentic. Deepfake technology creates similar concerns because it enables the production of fabricated audio-visual materials that appear authentic. A manipulated video portraying an individual making statements they never made, or a synthetic voice recording used to approve a transaction, affect the reliability of electronic records and create opportunities for deception. The difficulty lies in proving that the digital material was altered and connecting the alteration to the person responsible for the offence.

Sections 418 and 419 of the Criminal Code Act relating to fraud and false pretences remain relevant to identity-based misuse of deepfake technology. These provisions apply where offenders impersonate another person through digital means in order to deceive victims or obtain unlawful advantages (Obalola & Omotayo, 2021). The Supreme Court has explained the requirements for liability under section 419 of the Criminal Code Act in cases involving fraudulent representations where *In Onwudiwe v Federal Republic of Nigeria [2006] 10 NWLR (Pt. 988) 382*, the Court held that the prosecution must establish that a false representation was made, that the accused person made the representation, that the accused knew the representation was false or did not believe it to be true and that the representation was made with intent to defraud. These requirements correspond with the issues that arise where deepfake-generated representations are used to deceive victims. Deepfakes create new forms of impersonation because they allow offenders to reproduce facial features, voices and behavioural patterns of individuals.

A criminal uses a synthetic representation of a company executive, public official, or private individual to influence decisions or obtain confidential information. The existing provisions can address some of these acts, but they were not drafted with AI-generated impersonation in mind. This creates difficulties where the harm arises from the creation and circulation of synthetic content itself rather than from a traditional act of fraud. The offence of obtaining by false pretences under section 419 of the Criminal Code Act has relevance to deepfake-enabled financial deception. Fraudulent communications transmitted through emails, social media platforms and other electronic channels fall within the scope of this offence where the offender makes false representations that cause another person to part with money or property (Obalola & Omotayo, 2021) [30]. In *Elijah Okezie v The Queen [1963] 1 All NLR 1*, the Supreme Court considered the offence of obtaining by false pretences and affirmed that conviction requires proof of a false representation made with fraudulent intention and reliance by the victim resulting in the transfer of property. The principles established in the case remain applicable where synthetic audio, video, or digital communications are used to induce victims to surrender money or other valuable interests. Deepfake-generated messages and recordings increase the ability of offenders to present false information in a convincing manner. A synthetic voice resembling a business owner or family member persuade a victim to transfer funds or disclose sensitive information. The existing offence can address the fraudulent outcome, but it does not directly regulate the creation or distribution of deceptive AI-generated media.

2. The Penal Code Act

The Penal Code Act forms part of Nigerian criminal law framework applicable mainly in the northern states. Similar to the Criminal Code Act, it contains provisions addressing fraud, cheating, impersonation and false information. These offences apply to deepfake-related misconduct where synthetic content is used as a tool for deception or unlawful gain (Umejiaku & Anyaegbu, 2018) [67]. The Penal Code criminalises acts involving deception and fraudulent

representation. Deepfake technology facilitate cheating and personation by allowing offenders to assume another individual identity through fabricated audio, video, or images. A person who uses synthetic media to represent himself as another person for financial or personal advantage fall within existing criminal provisions. Nigerian courts have interpreted offences involving deception and dishonest inducement as requiring proof of fraudulent intention and reliance upon the false representation. In *Ibrahim v State [2015] 11 NWLR (Pt. 1471) 347*, the Supreme Court reiterated that offences involving dishonesty require proof of the accused person intention and the circumstances connecting the accused to the fraudulent conduct.

Enforcement Challenges in Regulating Deepfake Technology in Nigeria

1. Absence of Deepfake-Specific Legislation

Nigeria currently lacks legislation that specifically defines deepfake technology and criminalises harmful deepfake activities. Existing laws apply where deepfakes are used to commit recognised offences such as fraud, identity theft, cyber harassment, impersonation, or defamation, but these provisions do not address the full range of harms associated with synthetic media (Uba, 2021; Eguridu et al., 2024) [14, 66]. The absence of a dedicated offence creates uncertainty regarding which stage of the conduct attracts criminal liability. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 [11] does not expressly mention deepfakes, artificial intelligence-generated criminal activities, or several emerging technology-related offences. This limitation reflects the difficulty of maintaining legislation that remains effective as technology develops.

2. Difficulty in Applying Existing Cybercrime Laws to Deepfake Activities

Existing cybercrime laws create loopholes when they fail to address new forms of technological abuse (Onadeko and Afolayan, 2018). Eboibi (2019) [2, 25] identified difficulties arising from the inability of existing cybercrime laws to respond adequately to evolving digital practices. The judicial interpretation of cybercrime legislation in Nigeria demonstrates the difficulty of applying existing statutory provisions to technologically advanced offences. In *Julius v. Federal Republic of Nigeria [2021] LPELR-55390(CA)*, the Court of Appeal examined the prosecution of computer-related forgery under section 13 of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 [11]. The decision held that where legislation creates specific cyber offences, prosecutors must satisfy strict technical and evidential requirements before criminal liability can be established. This difficulty arises in deepfake cases where prosecutors must prove the creation, manipulation, authenticity, intent and distribution of synthetic content.

3. Uncertainty Regarding Criminal Responsibility for AI-Generated Content

Determining who should bear criminal responsibility for AI-generated content remains one of the difficult questions in deepfake regulation. Criminal liability traditionally depends on the existence of an unlawful act and a guilty mind. The concepts of *actus reus* and *mens rea* are designed around human conduct and intention, creating uncertainty regarding whether liability can be attributed directly to artificial intelligence or to persons who create, operate, or distribute AI-generated content (Eguridu *et al*., 2024; Hailtik & Afifah, 2024). Hallevy (2010) [14, 24, 26] proposed three models for addressing criminal responsibility involving artificial intelligence: the perpetration-via-another model, the natural-probable-consequence model and direct AI liability. Under current criminal law principles, Nigerian courts would likely face difficulties imposing direct criminal liability on AI systems.

4. Challenges in Establishing Attribution and Identifying Responsible Persons

The difficulty of identifying the responsible human actor is similar to challenges already recognised in Nigerian criminal law concerning attribution of unlawful online conduct. Nigerian courts require proof connecting the accused person to the prohibited act. In *FRN v. Ibori (2014)* [19] *1 NWLR [Pt. 1389] 1*, the Supreme Court reaffirmed that criminal liability requires proof of the elements of the offence against the accused person. The principle is relevant to deepfake offences because prosecution would require evidence linking the accused person to the creation, alteration, or distribution of synthetic content. Deepfake attribution is also affected by anonymity. Many deepfake creators conceal their identities, making it difficult for victims and authorities to identify responsible persons. The problem becomes more difficult when creators operate from foreign jurisdictions or distribute content through international platforms (Hall, 2018) [25].

Global Comparative Approaches to Deepfake Regulation and Lessons for Nigeria

1. The European Union Risk-Based Regulatory Model

The European Union Artificial Intelligence Act 2024[49] represents one of the first legislative attempts to regulate artificial intelligence through a dedicated legal framework. The Act recognises deepfake content as AI-generated or manipulated audio, image, video, or text material that resemble existing persons, objects, places, entities, or events and appear authentic to viewers (European Union Artificial Intelligence Act, 2024) [49]. The regulation places deepfakes in a transparency-based category rather than treating all deepfake applications as high-risk systems. Under Article 50 of the EU AI Act, providers and users of certain AI systems capable of generating synthetic content must disclose that the material has been artificially created or modified. The requirement applies particularly to AI-generated or manipulated audio, image and video materials that appear genuine. The objective is to allow individuals to distinguish authentic content from synthetic media and reduce the possibility of deception.

The classification of deepfakes under limited risk obligations has attracted criticism. Okoyenta (2025) [50] argues that the transparency requirements not adequately reflect the potential harm caused by malicious deepfake applications. The German Bundesrat also raised concerns regarding the failure of the EU AI Act to classify deceptive deepfakes as high-risk systems, arguing that inconsistent implementation among member states weaken protection and create regulatory uncertainty (Moreno, 2024) [42]. The EU approach is closely connected with broader European protection of privacy and personal data. Article 7 of the Charter of Fundamental Rights of the European Union protects private and family life, while Article 8 recognises

the right to personal data protection. These principles provide a legal foundation for addressing unauthorised use of personal images, voices and identity-related information in synthetic media production. The decision of the Court of Justice of the European Union in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014]* showed the relationship between digital technology and privacy protection. The Court examined whether search engine operators could be responsible for continued availability of personal information online. It recognised that individuals require protection against the continued dissemination of personal data where such publication interferes with privacy rights. The judgment established that technological platforms have responsibilities where their activities affect individual control over personal information.

The reasoning in Google Spain is relevant to deepfake regulation because deepfake production frequently involves the unauthorised use of personal images, voices and identity characteristics. A fabricated video portraying an individual performing an action that never occurred raises questions regarding control over personal identity and the responsibilities of platforms that enable distribution. European human rights jurisprudence has also addressed the relationship between privacy, dignity and expression. In *Von Hannover v Germany [No. 2]*, the European Court of Human Rights examined the conflict between freedom of expression and protection of private life. The Court recognised that private life extends beyond secrecy and includes elements relating to personal identity, reputation and personal development. This principle supports regulation of synthetic media where manipulation causes harm to dignity or reputation. *In S and Marper v United Kingdom [2008]*, the European Court of Human Rights considered the retention of biometric information by public authorities. The Court held that storage and use of personal information interfere with Article 8 rights where adequate safeguards are absent. The decision demonstrates that technological processing of personal information requires legal controls capable of protecting individual autonomy. The European experience demonstrates that deepfake regulation involves more than controlling technology. It requires legal protection for privacy, identity, dignity and reputation. For Nigeria, the EU model provides useful guidance on transparency obligations, authenticity verification and personal data protection. However, transparency obligations alone not address deliberate criminal misuse. Nigerian law requires specific offences targeting harmful creation, distribution and exploitation of deepfake materials.

2. The United States' Sectoral and State-Based Approach

The United States has adopted a fragmented approach to deepfake regulation based on constitutional principles, existing legal doctrines, federal proposals and state legislation. Unlike the European Union, the United States has not enacted a comprehensive federal statute governing deepfake technology. The American approach reflects the continuing balance between protection of freedom of expression under the First Amendment and prevention of harms involving privacy violations, fraud, identity exploitation and reputational injury. Deepfake regulation in the United States is influenced by the constitutional protection of speech. While the First Amendment protects expressive activity, it does not prevent legal responses to unlawful conduct involving deception, fraud, or exploitation of personal identity. Shannon (2020) [62] explains that individuals maintain privacy interests capable of restricting unauthorised use of their likeness or identity for harmful purposes. Before the introduction of deepfake-specific legislation, victims depended largely on existing civil remedies. American tort law provides possible claims involving intrusion upon seclusion, public disclosure of private facts, appropriation of name or likeness and false light publicity (Shannon, 2020) [62]. The appropriation doctrine is relevant where a person image or identity is used without consent, while false light claims apply where fabricated content creates a misleading impression about an individual.

These remedies have limitations because victims must satisfy existing legal requirements and demonstrate recognised harm. The rapid circulation of deepfake content through online platforms also make enforcement difficult because harmful material can reach large audiences before legal action is taken. Several US states have introduced targeted legislation addressing particular forms of deepfake abuse. Virginia criminalised the unlawful distribution of sexually explicit synthetic images involving identifiable individuals without consent through Virginia Code Annotated §18.2-386.2 (Loomis, 2022) [38]. The legislation addresses a form of abuse where artificial intelligence is used to create sexual representations of individuals who did not participate in the production of the material. Texas introduced Senate Bill 751 to regulate election-related deepfakes by prohibiting the creation or distribution of deceptive videos intended to influence an election or harm a candidate during a specified period before voting (KRW Lawyers, 2019) [8]. California adopted Assembly Bill 602 concerning sexually explicit deepfake material and Assembly Bill 730 addressing deceptive deepfake videos used during political campaigns (Lexology, 2020) [37].

At the federal level, several proposals have attempted to address deepfake-related harms such as the Malicious Deepfake Prohibition Act, Deepfake Accountability Act, Deepfake Report Act, NO FAKES Act and No AI Fraud Act (Miotti & Wasil, 2024) [40]. These proposals focus on issues such as unauthorised digital replicas, identity misuse, election interference and non-consensual synthetic content. The application of Section 230 of the Communications Decency Act remains a major issue in American deepfake regulation. Section 230 generally protects online platforms from liability for third-party content. Supporters argue that the provision supports online innovation, while critics maintain that it limits accountability where platforms facilitate harmful synthetic media distribution. The American experience provides lessons for Nigeria emphasizing that deepfake regulation require specific offences addressing particular harms rather than relying only on general cybercrime provisions.

3. China Deep Synthesis Regulatory Framework

China has adopted a direct regulatory approach to synthetic media through its Deep Synthesis Technology Regulation, which commenced operation on 10 January 2023 [28]. Unlike jurisdictions that rely mainly on existing privacy, criminal, or technology laws, China introduced specific obligations governing deep synthesis service providers and users. The

regulation was developed in response to concerns that synthetic media could be used for misinformation, identity manipulation, reputational harm and unlawful content distribution (Hemrajani, 2023) [28]. The Cyberspace Administration of China (CAC) supervises implementation of the regulatory framework and identifies risks associated with deep synthesis technologies such as the creation of false information, misuse of personal identity and interference with the dignity and reputation of individuals (Hemrajani, 2023) [28]. The Chinese model recognises that responsibility for deepfake-related harm involve both content creators and the technological systems that enable production and circulation.

The Deep Synthesis Technology Regulation places obligations on service providers offering AI-generated content tools. Providers are required to implement measures relating to user identity verification, security management, content monitoring and identification of synthetic materials. AI-generated content must contain indicators showing that it has been artificially created or modified, allowing users to distinguish synthetic media from authentic recordings (Kharpal, 2022; MKPO, 2025) [32, 41]. The regulation also places responsibilities on users who create, reproduce, publish, or distribute synthetic content. This approach reflects the view that deepfake harms arise through interaction between individuals, platforms and technological infrastructure. By assigning obligations to multiple actors, China seeks to reduce the possibility that harmful synthetic content can circulate without accountability. China regulatory framework extends beyond deep synthesis technology through wider governance measures for generative artificial intelligence. The Interim Measures for Generative Artificial Intelligence Services impose obligations relating to data protection, content management, accuracy requirements and compliance duties for AI service providers (MKPO, 2025) [41]. Providers must prevent unlawful content generation and take corrective action where violations occur.

The Chinese approach also demonstrates the importance of maintaining human responsibility in AI-supported decision-making. Chinese courts have introduced artificial intelligence tools for administrative tasks, electronic filing, legal research and document analysis, while maintaining that judicial decisions must remain under human control (MKPO, 2025) [41]. This approach recognises that artificial intelligence assists legal processes but should not replace judicial judgment. For Nigeria, the Chinese model provides lessons regarding provider responsibility, content traceability and cooperation between technology companies and enforcement authorities. Nigerian legislation requires AI service providers to verify users, preserve records relating to synthetic content creation, assist investigations and establish procedures for detecting harmful deepfake materials. However, regulatory adoption must reflect Nigerian constitutional environment where any deepfake framework should protect privacy, freedom of expression and due process while addressing harmful conduct. The Chinese model showed the value of direct regulation, but Nigerian implementation would require safeguards against excessive restrictions on lawful technological activities.

4. The United Kingdom Criminal Law and Online Safety Approach

The United Kingdom has adopted a combined approach involving criminal law, data protection principles and online platform regulation to address harms arising from digital technologies. The UK framework focuses on individual responsibility for misuse of technology and obligations imposed on digital platforms that facilitate the circulation of harmful content. The Computer Misuse Act (CMA) 1990[9] remains the principal legislation governing computer-related offences in the United Kingdom. The Act criminalises unauthorised access to computer material under section 1, unauthorised access with intent to commit further offences under section 2 and acts intended to impair computer systems under section 3 (Computer Misuse Act, 1990)[9]. Although enacted before the emergence of deepfake technology, the legislation demonstrates how existing criminal provisions apply to certain forms of technology-enabled misconduct. The interpretation of computer misuse offences was examined in *DPP v Lennon [2006]*, where the court considered unauthorised modification of computer systems under the Computer Misuse Act 1990 [9]. The decision demonstrates that existing criminal provisions apply to emerging technological conduct even where the specific method of misuse was not anticipated when legislation was enacted. The UK has introduced additional measures through the Online Safety Act 2023 [28], which establishes responsibilities for online service providers regarding harmful digital content. The legislation requires platforms to implement systems for identifying, reporting and addressing unlawful material distributed through their services (Devesh Kumar, 2025) [36]. This approach recognises that deepfake harms are amplified by online platforms that enable rapid dissemination.

The regulation of deepfake technology in the United Kingdom has focused particularly on non-consensual sexual imagery. Synthetic sexual content creates serious personal and reputational harm because victims be represented in explicit situations without permission. Earlier legal approaches created difficulties because prosecutors often had to establish specific intentions, such as causing distress, before securing convictions. Legislative reforms have sought to reduce these barriers and strengthen protection for victims (GOV.UK, 2022). The Online Safety Act 2023 [28] reflects a movement towards greater platform responsibility. Digital service providers be required to establish reporting mechanisms, assess risks and take measures to prevent unlawful content circulation (Devesh Kumar, 2025) [36]. This approach recognises that responsibility for digital harm extend beyond the individual who creates synthetic material.

United Kingdom judicial decisions have also examined the relationship between privacy, reputation and freedom of expression. In *Campbell v MGN Ltd [2004]*, the House of Lords considered the balance between freedom of expression and protection against misuse of private information. The decision established that personal privacy require protection where publication causes unjustified interference with individual autonomy. This principle is relevant to deepfake disputes involving fabricated representations of individuals. The responsibility of online intermediaries has also been examined in *Tamiz v Google Inc. [2013]*, where the Court of Appeal considered issues relating to defamatory material published through online platforms. The case illustrates the difficulties involved in determining responsibility between content creators and digital intermediaries. The UK experience provides lessons for Nigeria regarding the need for specific criminal offences, platform obligations and effective enforcement mechanisms.

Conclusion

Deepfake technology presents new challenges for Nigerian criminal law because existing legal rules were created before the rise of artificial intelligence-generated media. This study examined the ability of Nigerian laws to address harms arising from synthetic images, videos and audio materials. The Criminal Code Act, Penal Code Act and Cybercrimes Act provide possible remedies for some offences, but they do not directly regulate deepfake creation, distribution and misuse. Foreign approaches from the European Union, United States, China and United Kingdom show possible directions for legal reform in Nigeria. A suitable response requires clear offences for harmful deepfake activities, duties for technology providers, stronger digital evidence procedures and improved investigative capacity. Nigerian regulation must protect individuals from identity abuse, fraud and manipulation while allowing lawful uses of artificial intelligence tools. The development of deepfake laws will assist courts, investigators and victims in addressing digital deception and protecting trust in electronic evidence.

Recommendations

Based on the findings of the study, the following recommendations were made:

1. The National Assembly should enact comprehensive legislation specifically criminalising the malicious creation, distribution and use of deepfake content while providing clear rules on criminal liability, digital evidence and victim protection.
2. The Federal Government should strengthen the Cybercrimes (Prohibition, Prevention, etc.) Act and invest in advanced digital forensic infrastructure and specialised training for law enforcement agencies, prosecutors and judicial officers to improve the detection, investigation and prosecution of deepfake-related offences.
3. Artificial intelligence developers, social media platforms and digital service providers should be legally required to implement content authentication, watermarking, user verification and rapid takedown mechanisms to reduce the circulation of harmful synthetic media.
4. Nigeria should enhance international cooperation through mutual legal assistance, information sharing and cross-border enforcement partnerships to effectively investigate and prosecute transnational deepfake-related crimes

References

1. Adebayo v. State, 12 NWLR (Pt. 1421) 613 (2014).
2. Ajder H, Patrini G, Cavalli F, Cullen L. The state of deepfakes: Landscape, threats and impact. Deeptrace, 2019. https://docslib.org/download/12559428/the-state-of-deepfakes-landscape-threats-and-impact-henry-ajder-giorgio-patrini-francesco-cavalli-and-laurence-cullen-september-2019
3. Alanazi S, Asif S, Moulitsas I. Examining the societal impact and legislative requirements of deepfake technology: A comprehensive study. International Journal of Social Science and Humanity,2024:14(2):58-63. https://doi.org/10.18178/ijssh.2024.14.2.1194
4. Blakemore E. How photos became a weapon in Stalin Great Purge. History, 2020. https://www.history.com/articles/josef-stalin-great-purge-photo-retouching
5. Bourgault J. Free speech and synthetic lies: Deepfakes, synthetic media and the First Amendment. SJIPL,2025:3(1):50-73. https://digitalcommons.mainelaw.maine.edu/sjipl/vol3/iss1/5
6. Campbell v. Mirror Group Newspapers Ltd., [2004] UKHL 22. https://www.lawteacher.net/cases/campbell-v-mirror-group.php
7. Carpenter P. Faik: A practical guide to living in a world of deepfakes, disinformation and AI-generated deceptions. John Wiley & Sons, 2024.
8. Chesney R, Citron DK. Deep fakes: A looming challenge for privacy, democracy and national security. California Law Review,2019:107(6):1753-1820. https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security
9. Computer Misuse Act 1990 (UK). https://www.freeprivacypolicy.com/blog/computer-misuse-act-1990/
10. Constitution of the Federal Republic of Nigeria (1999, as amended).
11. Cybercrimes (Prohibition, Prevention, etc.) Act (2015).
12. DPP v. Lennon, EWHC 1201 (Admin) (2006). https://www.bailii.org/ew/cases/EWHC/Admin/2006/1201.html
13. Eboibi FE. A critical exposition of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act 2015. Delta State University Law Review, 2019, 5(1). https://delsulawreview.com/wp-content/uploads/2023/07/3.-A-Critical-Exposition-Of-The-Nigerian-Cybercrimes-Prohibition-Prevention-Etc-Act-2015.pdf
14. Eguridu H, Tolani T, Olusola O, Sakpere W. Impact of information technology on civil rights and criminal liabilities. African Journal of Law, Ethics and Education,2024:7(1):55-68. https://ajleejournal.com/index.php/ajlee/article/view/168
15. Eigbedion A. Deepfakes: Legal & regulatory considerations in Nigeria. SSRN, 2020. https://ssrn.com/abstract=3670644
16. Elijah Okezie v. The Queen, FSC 36/1962, [1963] NGSC 2 (January 4, 1963). https://nigerialii.org/akn/ng/judgment/ngsc/1963/2/eng@1963-01-04
17. European Court of Human Rights. Von Hannover v. Germany (No. 2), Applications Nos. 40660/08 and 60641/08, Judgment of February 7, 2012. 2012. https://hudoc.echr.coe.int/eng?i=001-109029
18. Federal Republic of Nigeria. Constitution of the Federal Republic of Nigeria (as amended). 1999.
19. Federal Republic of Nigeria v. Ibori, 1 NWLR (Pt. 1389) 1 (2014).
20. Federal Republic of Nigeria v. James Onanefe Ibori & Ors, 1 NWLR (Pt. 1389) 1 (2014).
21. Fehintola IJ. An appraisal of the prospects and challenges of cybercrime investigation and prosecution in Nigeria (Master's thesis, Crescent University, Abeokuta), 2023.
22. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja

González (2014). https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/
23. GOV.UK. New laws to better protect victims from abuse of intimate images. 2022 Nov 25. https://www.gov.uk/government/news/new-laws-to-better-protect-victims-from-abuse-of-intimate-images
24. Hailtik AGE, Afifah W. Criminal responsibility of artificial intelligence committing deepfake crimes in Indonesia. Asian Journal of Social and Humanities,2024:2(4):776-795. https://doi.org/10.59888/ajosh.v2i4.222
25. Hall HK. Deepfake videos: When seeing isn't believing. Catholic University Journal of Law and Technology,2018:27(1):51-75. https://scholarship.law.edu/jlt/vol27/iss1/4
26. Hallevy G. The criminal liability of artificial intelligence entities from science fiction to legal social control. Akron Intellectual Property Journal,2010:4(2):1. https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1
27. Heidari A, Navimipour NJ, Dağ H, Unal M. Deepfake detection using deep learning methods: A systematic and comprehensive review. WIREs Data Mining and Knowledge Discovery,2024:14(2):e1520. https://www.scilynk.com/paper/W4388851105
28. Hemrajani A. China's new legislation on deepfakes: Should the rest of Asia follow suit? The Diplomat, 2023 Mar 8. https://thediplomat.com/2023/03/chinas-new-legislation-on-deepfakes-should-the-rest-of-asia-follow-suit/
29. Julius v. FRN, (2021) LPELR-54201(CA). https://lawcarenigeria.com/julius-v-frn-2021/
30. Karasavva V, Noorbhai A. The real threat of deepfake pornography: A review of Canadian policy. Cyberpsychology, Behavior, and Social Networking,2021:24(3):203-209. https://doi.org/10.1089/cyber.2020.0272
31. Kertysova K. Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated and can be countered. Security and Human Rights,2018:29(1-4):55-81. https://www.shrmonitor.org/assets/uploads/2019/11/SHRM-Kertysova.pdf
32. Kharpal A. China is about to get tougher on deep fakes in an unprecedented way. Here's what the rules mean. CNBC, 2022 Dec 22. Retrieved July 4, 2026, from https://www.cnbc.com/amp/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes-html
33. Kietzmann J, Lee LW, McCarthy IP, Kietzmann TC. Deepfakes: Trick or treat? Business Horizons,2020:63(2):135-146. https://doi.org/10.1016/j.bushor.2019.11.006
34. KRW Lawyers. 'Deep fake' videos under spotlight of new Texas law. 2019 Nov 13. https://www.krwlawyers.com/2019/11/13/deepfake-videos-under-spotlight-of-new-texas-law/
35. Kshetri N. The economics of deepfakes. Computer,2023:56(8):89-94. https://www.computer.org/csdl/magazine/co/2023/08/10206053/1PlcMAFEiNa
36. Kumar D. Deepfakes, free speech and the right to truth: A comparative legal study on regulating synthetic media in the USA, UK and India. Advanced International Journal for Research (AIJFR),2025:6(4):1-11. https://www.aijfr.com/papers/2025/4/1117.pdf
37. Lexology. California deepfake law first in country to take effect. 2020 Jan 20. https://www.lexology.com/library/detail.aspx?g=4700f977-4845-417b-834d-b3c06390ee27
38. Loomis A. Deepfakes and American law. Davis Political Review, 2022 Apr 20. https://www.davispoliticalreview.com/article/deepfakes-and-american-law
39. Meskys E, Liaudanskas A, Kalpokiene J, Jurcys P. Regulating deep fakes: Legal and ethical considerations. Journal of Intellectual Property Law & Practice,2020:15(1):24-31. https://doi.org/10.1093/jiplp/jpz167
40. Miotti A, Wasil A. Combatting deepfakes: Policies to address national security threats and rights violations (arXiv:2402.09581). arXiv, 2024. https://arxiv.org/abs/2402.09581
41. Mkpo DC. Is truth and integrity of justice on trial in the age of artificial intelligence (AI)? Re-assessing digital evidence in the context of AI-generated evidence such as deepfakes. International Review of Law and Jurisprudence, 2025, 7(1). https://www.nigerianjournalsonline.org/index.php/IRLJ/article/view/1710
42. Moreno F. Generative AI and deepfakes: A human rights approach to tackling harmful content. International Review of Law and Computer Technology, 2024, 38(3). https://www.tandfonline.com
43. Musa Ibrahim v. The State, SC. 652/2013, NGSC 26 (May 4, 2017).
44. Nnamdi N, Oniyinde O, Abegunde B. An appraisal of the implications of deep fakes: The need for urgent international legislations. American Journal of Leadership and Governance,2023:8(1):44. https://www.ajpojournals.org
45. NVIDIA. What is generative AI? 2024. https://www.nvidia.com/en-us/glossary/generative-ai/
46. Obalola AO, Omotayo FA. Cybersecurity and legal framework in Nigeria: Analysis of the Cybercrime Act 2015. African Journal of Law & ICT,2021:9(2):45-63.
47. Oboh EN. The facts and mirage of integrating artificial intelligence into the judicial system of Nigeria. Wukari International Studies Journal,2025:9(2):115-124. https://www.researchgate.net/publication/395694986_The_Facts_and_Mirage_of_Integrating_Artificial_Intelligence_into_the_Judicial_System_of_Nigeria
48. Ogana E. An analysis of legal framework on combating cybercrime in Nigeria (Master's dissertation, Ahmadu Bello University, Zaria), 2017.
49. Okeke AO, Nwosu CJ, Asogwa J, Dada O. Utilization of deepfake technology in the film industry: Analysing AI-generated performances in the Hollywood film The Irishman and its impact on artistic integrity. Scholarly Journal of Social Sciences Research,2024:3(6):35-51. https://doi.org/10.5281/zenodo.13989607
50. Okoyenta S. Appraisal of the implications of deepfake technology in litigation. SSRN, 2025. https://ssrn.com/abstract=5160259

51. Olasiyan TT, Olasiyan AF. Regulating synthetic identity: Deepfakes, voice-cloning and the future of AI law. SSRN, 2026. https://ssrn.com
52. Onadeko OA, Afolayan AF. A critical appraisal of the Cybercrimes Act 2015 in Nigeria. International Society for Reform of Criminal Law (ISRCL), 2018. https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf
53. Onwudiwe v. Federal Republic of Nigeria, (2006) 10 NWLR (Pt. 988) 382.
54. Pawelec M. Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. Digital Society,2022:1(1):Article 19. https://doi.org/10.1007/s44206-022-00010-6
55. R v. John Ogbuewu, 12 WACA 483 (West African Court of Appeal 1949).
56. Raymond Akolo Julius v. Federal Republic of Nigeria, LPELR-54201 (CA) (2021). https://lawcarenigeria.com/julius-v-frn-2021/
57. Russell SJ, Norvig P. Artificial intelligence: A modern approach. 3rd ed. Pearson; 2016.
58. Ryman-Tubb NF, Krause P, Garn W. How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Engineering Applications of Artificial Intelligence,2018:76:130-148. https://doi.org/10.1016/j.engappai.2018.07.008
59. S. and Marper v. United Kingdom, Application Nos. 30562/04 and 30566/04 (European Court of Human Rights, December 4, 2008). https://hudoc.echr.coe.int/eng?i=001-90051
60. Sample I. What are deepfakes - and how you can spot them. The Guardian, 2020 Jan 13. https://www.theguardian.com
61. Sekoni-Dairo RA. Deepfakes, consent and the law in Nigeria: The urgent need for regulation. SSRN, 2026. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6654678
62. Shannon R. The deepfake dilemma: Reconciling privacy and First Amendment protections. SSRN, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3636464
63. Sullivan-Paul M. How would ChatGPT vote in a federal election? A study exploring algorithmic political bias in artificial intelligence (Doctoral dissertation, School of Public Policy, University of Tokyo), 2023.
64. Tamiz v. Google Inc., [2013] EWCA Civ 68 (Court of Appeal of England and Wales).
65. Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J. Deepfakes and beyond: A survey of face manipulation and fake detection. Information Fusion,2020:64:131-148. https://doi.org/10.1016/j.inffus.2020.06.014
66. Uba J. Deepfakes in Nigeria: Protection and legal framework against deepfake attacks in Nigeria. Olisa Agbakoba Legal, 2021 Sep 23. https://oal.law/deepfakes-in-nigeria-protection-and-legal-framework-against-deepfake-attacks-in-nigeria/
67. Umejiaku NO, Anyaegbu MI. Legal framework for the enforcement of cyber law and cyber ethics in Nigeria. International Journal of Computers & Technology,2018:15(10):1-10.
68. Von Eschenbach WJ. Transparency and the black box problem: Why we do not trust AI. Philosophy & Technology,2021:34(4):1607-1622.
69. Von Hannover v. Germany (No. 2), Application Nos. 40660/08 and 60641/08 (European Court of Human Rights, February 7, 2012). https://hudoc.echr.coe.int/eng?i=001-109029
70. Westerlund M. The emergence of deepfake technology: A review. Technology Innovation Management Review,2019:9(11):39-52. https://doi.org/10.22215/TIMREVIEW/1282