ISSN: 2755-6190

Review Article

Open Access Journal of Artificial Intelligence and Technology

Ai, Deepfakes And Ar: Emerging Legal Frontiers In Media And Telecommunications

Toluwanimi Festus Olusola

A 500-level student of the Faculty of Law, Lead City University, Ibadan

Corresponding author
Toluwanimi Festus Olusola, A 500-level student of the Faculty of Law, Lead City University, Ibadan.

Received: March 07, 2026; **Accepted:** March 18, 2026; **Published:** March 25, 2026

ABSTRACT

Artificial Intelligence (AI) has significantly transformed the landscape of digital media and telecommunications by enabling advanced forms of content creation and manipulation. Technologies such as deepfakes, synthetic voices, and augmented reality (AR) have expanded the possibilities of communication, entertainment, and information dissemination. While these innovations provide remarkable opportunities for creativity, efficiency, and enhanced user interaction, they simultaneously introduce complex legal, ethical, and societal challenges. This paper examines the intersection of AI, AR, and deepfake technologies within the media and telecommunications sector, with particular focus on the regulatory responses developed at international, regional, and domestic levels. It evaluates global initiatives such as the UNESCO Recommendation on the Ethics of Artificial Intelligence and the European Union's AI Act, alongside regional efforts like the African Union's AI Strategy and domestic regulatory approaches in jurisdictions including the United States, India, and Nigeria. The study further explores key legal issues arising from these technologies, including privacy and consent, intellectual property ownership, cyberbullying, defamation, and the spread of misinformation. Particular attention is given to the implications of these challenges for democratic integrity and public trust in digital communications. The paper concludes by proposing regulatory improvements, including stronger institutional oversight, international technological cooperation, capacity-building for detecting AI-generated content, and public education initiatives aimed at mitigating the risks associated with emerging digital technologies.

Introduction

Artificial Intelligence (AI), has had a profound impact on a variety of domains that make up the digital media and communications terrain by ushering in a transformative era in media creation, and communications; offering unparalleled capabilities to manipulate and fabricate digital content with Technologies such as deepfakes, synthetic voices, virtual realities, and augmented realities [1].

However, these digital capabilities have come with uncertainties, and high risks [2]. Nonetheless, outrightly discarding the boons derived from these technological advancements is not the next point of call. It rather becomes imperative for the legal framework to be refined to contain and manage these ever-growing advancements [3].

Artificial Intelligence

As has been the case with similar concepts of a multi-faceted nature, adopting a universal definition of AI has been challenging. Hence, there really has been no single definition that captures an array of technologies that could be termed AI [4].

Nonetheless, the OECD defines an AI system as a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives through the use of machines and/or human-based data and inputs [5].

In Addition, According To The European Parliament

AI is the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity. AI enables technical systems to perceive their environment, deal with what they perceive, solve problems and act to achieve a specific goal [6].

AI is seen causing unconventional developments in industries such as advertising, and entertainment; leveraging on the synthetic media for positive outcomes [7]. These developments are exemplified by self-driving cars, super-human performance in games, human-level spoken interaction, intelligent robots, creation of cures to diseases [8]. In rem, they range from day-to-day use (like Amazon's Alexa to Google maps), to more sophisticated devices (like Tesla's self-driving) [9].

Citation: Toluwanimi Festus Olusola. Ai, Deepfakes And Ar: Emerging Legal Frontiers In Media And Telecommunications. Open Access J Artif Intel Tech. 2026. 2(1): 1-5. DOI: doi.org/10.61440/OAJAIT.2026.v2.26

Deepfakes

The European Union's Artificial Intelligence Act defines a "Deepfake" as an;

AI-generated or manipulated image, audio, or video content that mimics existing persons, objects, places, or other entities or events, creating a false appearance of authenticity or truthfulness to viewers. Deepfakes generally refer to a form of technology that creates realistic videos, images, and audio by using sophisticated Artificial Intelligence (AI), Photoshop, and machine learning algorithms [especially the generative adversarial networks (GANs)] to overlay a person's voice or face onto someone else's body and speech in a bid to create convincing replica of videos and audio clips [10-12].

Augmented Reality (Ar)

AR uses the concept of a virtual environment where human senses (vision, haptics, hearing, smell, etc.) are controlled by a computer, and adds visible digital content to a person's perception of the real world [13,14]. AR integrates synthetic information (which can be in 2D and/or 3D graphical elements) into real environments [15]. Examples include the likes of Google Glass, Google Map, Pokémon Go, Google's ARCore and Apple's ARKit [16,17].

Ai, Ar, And Deepfakes In Media And Telecommunications

The most attention-seeking was that created by a filmmaker; Jordan Peele in 2018 which was a deepfake video of former US President Barack Obama delivering a fictional public service announcement to warn about the potential dangers of deepfake technology. This raised concerns about the erosion of trust in media and the spread of misinformation [18].

Deep fake has also been used in Nigeria to create a conversation between Peter Obi and Bishop Oyedepo in 2023 in a bid to discredit Peter Obi on media platforms, and to exploit the available telecommunications media [19].

Augmented Reality on a different is made up of the camera (including sensor), projection, and reflection [20]. This has helped ttelecommunications companies leverage augmented reality to enhance teleconferencing, customer service, spatial computing, and navigation; which has made it offer features like enhanced real-time communication, improved training, seamless integration, and increased productivity [21,22]. These technological advancements are strongly connected with the media and telecommunications (especially social media which serves both as a media ground and means of telegraphic communications) since the text, images, videos, sound being created, and altered are the key elements of interaction and communication within the public sphere [23,24].

Key Regulations On Ai, Ar And Deepfake In Media And Telecommunications

The United Nations (UN) has recognized the importance of AI governance and ethics, and has called on international cooperation to tackle the risks that arise from these technological advancements on the use of AI [25].

The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) provides the first global guidance on the ethical use of AI, advocating for transparency, accountability, and fairness [26]. Regionally, the European Union has been at the forefront of regulating artificial intelligence. This is depicted through the European Union's General Data Protection Regulation (GDPR) which provides mechanisms to combat unauthorized use of personal data. Again, the EU established the AI Act (2024) which seeks to establish comprehensive guidelines for the use of AI systems. Other measures include the likes of the Digital Services Act (DSA), the Digital Markets Act (DMA), and the Audiovisual Media Services Directive [27].

For Africa, the AU Strategy on Artificial Intelligence (AI) was adopted by the AU Executive Council during its 45th Ordinary Session held on to 18th – 19th July 2024, in Accra, The Republic of Ghana with a view to achieving the positive and transformative potential for African development and mitigate potential risks [28]. Domestically, in analysing civil law jurisdictions, we examine the United States' approach to regulating deepfakes in the US as disjointed and fragmented, varying widely by state but they still attempt to guard against negative use of these technological advancements [29].

In examining common law jurisdictions, we examine India where the legal framework to deal with deepfakes is still in its infancy. Nonetheless, the Indian Information Technology Act (2000), and the Indian Penal Code (IPC) are used as legal frameworks to prosecute the offences that are related to this technology. For instance, Section 67A of Indian Information Technology Act, makes it unlawful to publish nonconsensual pornographic content, and section 66C punishes identity.

In Nigeria, these levels of technology are yet to be met with gainful, and specially-directed laws to combat the ills that may be presented by these technological advancements. Nonetheless, the Nigerian Cybercrimes (Prohibition and Prevention etc.) Act, 2015 deals with certain aspects that deal with the use of the creation of these tools to bully or manipulate persons. The use and processing of data (especially by AR) is also regulated by the Nigeria Data Protection Act with a view to ensure the privacy and protection of personal data.

Key Issues Surrounding Ai, Ar And Deepfake In Media And Telecommunications

It must be noted that the widespread availability of these tools has also resulted in ethical, legal, and societal challenges that are yet to be fully addressed including [30]

Privacy and Consent

AR in particular relies upon the prospect of recording and analyzing the physical world in or near real time, and therefore presents a particularly acute example of a broader trend toward information collection, processing, and dissemination; as it processed the likes of biometric data, location tracking, and behavioral patterns [31]. This then raises concerns on privacy, and lack of consent (among the most pressing legal concerns associated with these technological advancements). This is as a result of the non-consensual data that may be processed by the AR technology, and the non-consensual pornographic deepfakes that disproportionately target women and have devastating consequences for their victims [32].

Even though the available laws seek to combat the issues of privacy and consent, the enforcement of privacy laws remains challenging, particularly in the digital age, where anonymity and cross-border platforms complicate accountability [33].

Intellectual Property

Deepfake and AI media produce a host of questions centred around the issues of intellectual property such as whether AI-generated media is copyrightable and in whom such incorporeal right is vested. The United States leads in clarification of this issue as may be seen in its judicial decision in Thaler v. Perlmutter wherein the court upheld that a piece of art generated from an AI program with no human involvement does not qualify for human authorship; thus, not eligible for protection [34].

Nonetheless, when an AI is used as a tool by a human creator the resulting work may qualify for protection which raises the question of the extent of human involvement needed to qualify for copyright protection.

On a different end of the same table, these technological devices may run contrary to an IP holder's right to grants creators exclusive rights to their original works, such as writing, music, or software. This is because these distributions or modifications of such protected material without permission from the IP right holder would amount to a violation.

AR technologies on a different hand, quite literally blur the lines between physical and digital assets, and therefore creating complex intellectual property on the ownership of the virtual creations, and digital Counterfeiting of virtual goods, such as in-game items or NFTs (non-fungible tokens) [35,36].

Cyberbullying, Defamation and Misinformation

Deepfakes have been used to create false and damaging representations of individuals, leading to defamation claims [37]. The use of deepfakes in spreading political misinformation further complicates matters, raising concerns about the integrity of democratic processes as seen in the Nigerian example of Peter Obi above.

These creations may also be used on online platforms, social media, chat rooms, text messages, to spread rumours, or cause emotional distress [38]. Pornographic deepfakes can be used to threaten, intimidate, and cause psychological harm; reducing victims to sexual objects, inflicting mental misery as well as financial loss and collateral repercussions such as job loss in some circumstances [39,40].

They then become defamatory when these false or misleading creations damage a person's reputation and brings shame to a person in the eyes of the common man [41].

More so, this deepfakes can be weaponized through AR to spread disinformation, impersonate public officials, or incite panic [42]. Hence, the risks posed by these technological advancements are not just individual problems. It is for this reason that legal frameworks must begin to address these risks while safeguarding freedom of speech and expression [43]. In the grand scheme of things, this may lead to acts like disrupting critical digital infrastructure, stealing sensitive data, or launching cyberattacks to cause widespread damage and threaten or inflict harm [44].

Recommendations For Regulatory Improvements

The following recommendations are made in view of suggesting measures for strengthening existing regulatory frameworks, and creating new ones:

Subjecting Approval Of Sensitive Innovations To Specialized Bodies

It is recommended that technological innovations that may be of sensitive effects (especially those that may be public consumption) be subjected to technical bodies (such as Nigeria's NITDA) for approval before dispersion. Such approvals may also require full disclosure of creation process (just as is done for patent applications) or requirement of availability of reversal effects. This would ensure that persons are not irredeemably jeopardized by these innovations.

Continued Sharing of Innovation Amongst Nations

While deepfakes remain tremendous threats to many aspects of existence, the likes of OpenAI's release of text-to-video generative AI, and Sora counteract such risks by their reversal capabilities. However, some of these innovations are only available in some jurisdictions [45,46]. This in itself means that countries must continue to share innovations to help one another.

Establishing Trainings For Recognizing Ai Creations.

In 2019, Facebook, Microsoft, Amazon Web Services, and many institutions launched a competition in to develop deepfake detection capabilities, and at the conclusion of same, the winning team was able to accurately recognize deepfakes 65%of the time [47]. This goes to show that beyond the counteractive innovations above, humans can be trained to learn these things [48], and this would water-down the ripple-effects of these innovations at crucial points.

Education And Awareness Initiatives

The trainings noted above may come in form of institutional or governmental investments which may then be employed to educate the general public and reduce the destructive tendencies of these innovations.

More so, comprehensive education and awareness initiatives may be launched to enable individuals and organizations recognize and respond to threats related to disinformation [49]. These can mitigate the impact of third-party cybersecurity risks on free speech, privacy, and disinformation.

Conclusion

The rapid advancement of Artificial Intelligence (AI), deepfakes, and augmented reality (AR) has significantly reshaped the media and telecommunications landscape. These technologies have created new opportunities for innovation, communication, and digital creativity, enabling more immersive and efficient interactions across industries such as entertainment, advertising, and information dissemination. However, their growing use has also generated complex legal, ethical, and societal challenges that cannot be ignored. Deepfakes, for instance, have demonstrated the ability to manipulate audio-visual content in ways that may spread misinformation, damage reputations, and undermine

public trust in digital media. Similarly, AR technologies raise concerns regarding privacy, data protection, and the unauthorized processing of personal and environmental information.

Despite these risks, rejecting these technologies entirely would hinder technological progress and innovation. Instead, the focus should be on developing effective legal and regulatory frameworks that balance technological advancement with the protection of fundamental rights. While international and regional initiatives have begun addressing these issues, many jurisdictions, including Nigeria, still rely largely on existing cybercrime and data protection laws that only partially address the emerging risks. Strengthening regulatory oversight, promoting technological cooperation, and investing in public awareness and digital literacy will be essential in ensuring that these technologies are used responsibly while preserving trust in digital communications.

References

1. Stamatis Karnouskos. 'Artificial Intelligence in Digital Media: The Era of Deepfakes' IEEE Transactions On Technology And Society. 2020. 1: 138-147.
2. Mark Greaves. "'Deepfakes' ranked as most serious AI crime threat". 2020.
3. Westerlund M. 'The emergence of deepfake technology: A review' (2019) Technology Innovation Management Review. 2019. 9: 39-52.
4. Emmanuel Salami, Iheanyi Nwankwo. 'Regulating the privacy aspects of artificial intelligence systems in Nigeria: A primer'. 2020. 1.
5. OECD. 'OECD AI principles overview'. 2025.
6. European Parliament, 'What is artificial intelligence and how is it used?' NEWS. 2023.
7. Mou Y, Xu K. 'The media inequality: Comparing the initial human-human and human-AI social interactions' Computers in Human Behavior. 2017. 72 : 432-440.
8. Karnouskos S.'Self-driving car acceptance and the role of ethics' (2020) IEEE Transactions on Engineering Management. 2020. 67: 252-265.
9. Marcus Okoko, Co. 'Robot Rights: The Legal Impacts Of Artificial Intelligence'. 2022.
10. Aldrin Kolakkal. 'Deep Fake Technology: Analysis of Legal Framework and The Way Forward' The Indian Journal For Research In Law And Management. 2024. 1.
11. Ganesh Subramanian, Swathi S. 'The Legal Dilemma of Deepfakes Ai Liability and the Challenges of Digital Identity Theft' International Journal for Multidisciplinary Research (IJFMR). 2024. 6.
12. Komal Ahuja. 'The Legal Status of Deepfakes and AI-Generated Media'. 2025.
13. Mark A. Lemley and others, 'Law, Virtual Reality, and Augmented Reality' University of Pennsylvania Law Review. 2018. 166.
14. Oliver Bimber Raskar, Ramesh, Spatial Augmented Reality: Merging Real and Virtual Worlds. 2005.
15. Ronald Azuma T. 'A survey of augmented reality' (1997) Teleoperators and Virtual Environments. 1997. 6: 355-385.
16. Akinsuru Adedoyin, Olaoba Joy. 'Augmented and Virtual Reality: Defining Legal Boundaries and Responsibilities'. 2025.
17. Nishith Desai Associates, 'Augmented, Virtual and Mixed Reality– A Reflective Future Legal, Regulatory and Tax Considerations Strategic, Legal, Tax and Ethical Issues'. 2019.
18. Shahana Fatima, 'Legal and Ethical Implications of Deepfake Technology: Exploring the Intersection of Free Speech, Privacy, and Disinformation'. 2025.
19. Duale, Ovia, Alex-Adedipe.'Deepfakes: Legal Safeguards in Nigeria'. 2025.
20. Masitoh Indriani and Liah Basuki Anggraeni, 'What Augmented Reality Would Face Today? The Legal Challenges to the Protection of Intellectual Property in Virtual Space'. 2022. 5.
21. Muye Lin, Kangyu Yang. 'Breakthroughs and Applications of Augmented Reality (AR) Technology in the Digital Media Field'. Applied Mathematics and Nonlinear Sciences. 2024. 9: 1-17.
22. Grady Andersen.'Telecommunications and Augmented Reality: Transforming Communication Channels'. 2024.
23. Gabe Regan, 'A Brief History of Deepfakes'. 2024.
24. Miletskiy VP, Cherezov DN, Strogetskaya EV. 'Transformations of professional political communications in the digital society (by the example of the fake news communication strategy)'. Communication Strategies in Digital Society Workshop (ComSDS) IEEE. 2019.
25. United Nations System. 'United Nations system white paper on artificial intelligence governance: an analysis of current institutional models and related functions and existing international normative frameworks within the United Nations system that are applicable to artificial intelligence governance'. 2024.
26. SHS/BIO/PI/2021/1.
27. Arpita Ranjan, Aman Yadava.'Artificial Intelligence in the Legal Sector: Opportunities, Challenges, and Regulatory Perspectives' International Journal Of Human Rights Law Review. 2024. 3.
28. Arican Union. 'Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity'. 2024.
29. Yinuo Geng. Comparing 'Deepfake" Regulatory Regimes in the United States, The European Union, And China'. Georgetown Law Technology Review. 2023. 7.
30. Ketty Anderson, 'Legal And Regulatory Frameworks For Ai-Generated'. 2024.
31. Franziska Roesner, and others, 'Augmented Reality: Hard Problems of Law and Policy'. 2014.
32. Singh Jaswinder. 'The Rise of Synthetic Data: Enhancing AI and Machine Learning Model Training to Address Data Scarcity and Mitigate Privacy Risks' (2021) Journal of Artificial Intelligence Research and Applications. 2021. 1: 292-332.
33. Firth J, Johnston L. 'Privacy in Virtual Spaces: Challenges and Opportunities'. Journal of Information Technology. 2019. 34: 450-472.
34. No. 23-5233 (D.C. Cir. 2025).
35. Rhonda Hadi, Eric S. Park, 'Bridging the digital and physical: The psychology of augmented reality' (2024) Current Opinion in Psychology. 2024. 58.
36. Brian Wassom D. Augmented Reality Law, Privacy, and Ethics: Law, Society, and Emerging AR Technologies. 2014.

37. Chesney R Citron D. 'Deepfakes and the new disinformation war: The coming age of post-truth geopolitics'. Foreign Affairs. 2019. 98: 147-153.
38. Saddam Hossain Mukta MD. 'An Investigation of the Effectiveness of Deepfake Models and Tools' Journal of Sensor and Actuator Networks. 2023. 12.
39. Lenhart A, Ybarra M, Price-Feeney M. 'Nonconsensual image sharing: One in 25 americans has been a victim of "revenge porn' (Data & Society Research Institute, and Center for Innovative Public Health Research. 2016.
40. Ashish Jaiman. 'The Danger of Deepfakes'. 2023.
41. Jia Wen Seow. and others, 'A Comprehensive Overview of Deepfake: Generation, Detection, Datasets and Opportunities'. 2022. 513: 351-371.
42. Singh Jaswinder. 'Deepfakes: The Threat to Data Authenticity and Public Trust in the Age of AI-Driven Manipulation of Visual and Audio Conten'. Journal of AI-Assisted Scientific Discovery. 2022. 2: 428-467.
43. Anna Maria Collard. '4 Ways to Future-Proof Against Deepfakes in 2024 and Beyond'. 2024.
44. Arslan F. 'Deepfake Technology: A Criminological Literature Review' (2023) Sakarya Üniversitesi Hukuk Fakültesi Dergisi/Sakarya Hukuk Dergisi. 2023. 11: 701-720.
45. Jia Y, 'Transfer learning from speaker verification to multispeaker text-to-speech synthesis'. 2018.
46. Rachel Curry. 'AI deepfakes are poised to enter court proceedings at time of low trust in legal system'. 2024.
47. Jeremy Kahn. 'Facebook contest shows just how hard it is to detect deepfakes' Fortune. 2020.
48. Maras MH, Alexandrou A. 'Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos'. The International Journal of Evidence & Proof . 2018. 23: 255-262.
49. Horn S, Veermans K. 'Critical thinking efficacy and transfer skills defend against 'fake news' at an international school in finland' (2019) Journal of Research in International Education. 2019. 18: 23-41.