AN ANALYTICAL STUDY ON THE INTERSECTION OF AI-GENERATED CONTENT AND INTELLECTUAL PROPERTY RIGHTS IN INDIA

Kinkini Chakraborty, LLM, Christ University, Bangalore Central Campus

ABSTRACT

Traditional intellectual property (IP) frameworks now face several difficulties as a result of the swift growth of artificial intelligence (AI), especially with regard to authorship, ownership, and liability for works produced by AI. The quest to employ artificial intelligence in every area of knowledge, including our personal settings, has been sparked by the continuous development of technology. Mostly abbreviated as "AI," artificial intelligence (AI) is a general term used for a wide range of applications at various levels of human participation. Artificial intelligence has mastered the art of personalising us in the digital realm. One of these ways to trick people using AI is called "deepfakes," in which machine learning algorithms—more especially, generative adversarial networks, or GANs—are used to create artificial media that looks like people but has some content altered. At the core of artificial intelligence is deepfake technology, which is quickly taking over various social media channels. This rapid development compels us to examine the legal aspects of deepfakes. Examining how deepfakes affect cyber law, intellectual property law, and defamation law reveals the various legal complexities surrounding this technology. In this article, the disruptive nature of deepfakes, their manifestations and effects, the recipients of the AI technology and their rights—such as the right to publicity and personality—as well as potential threats and possible legal remedies within the framework of intellectual property law are reviewed and analysed.

Keywords: Intellectual Property Rights, Artificial Intelligence, Deepfake, Legal Aspects, Privacy breach.

INTRODUCTION

AI has produced transformative tools capable of generating media that is very realistic and convincing, often indistinguishable from that produced by a human. These are synthetic media frequently referred to as "deepfakes," which are artificial media generated through various machine learning approaches, which is an achievement in and of itself. While there is exciting potential for deepfakes in the entertainment, education, and creative industries, the ability to generate sexually explicit content as well as generate non-consensual content creates serious question and debate related to intellectual property rights, privacy, and human dignity.

Intellectual property law is fundamentally based on the concepts of promoting creativity and protecting ownership. However, when AI autonomously creates images, video, or audio that look like real persons, the existing framework has difficulty dealing with issues related to authorship, originality, and infringement. This problem is exacerbated in instances of explicit or pornographic deepfakes where a person's likeness is digitally reproduced without permission. This abusive use of deepfake technologies undermines personal autonomy and moral rights, as well as unsettles the traditional theories of copyright, trademark, and publicity rights. This study plans to consider the relationship between AI-created deepfake media and intellectual property rights, with emphasis on explicit material. It will explore if and how current legal doctrines address the unauthorized creation or distribution of explicit content, and ultimately, it will look into causation related to the attribution of liability - for example, some technologies may create content where there is little human involvement. This study will analyze case law, legislation from the United States and elsewhere, and will evaluate judicial trends and legislative possibilities in an effort to expose gaps in protection for policy objectives that reconcile innovation, individual rights, and society's safety. This analytical project aims to resolve these tensions by exploring the intersection of intellectual property rights and deepfake technology, with a specific emphasis on explicit media and content. Specifically, this would include analyzing a) whether copyright law can adequately deal with the originality and authorship questions raised by deepfake technology, b) how moral and publicity rights can be used to protect individuals from non-consensual exploitation, and c) whether the international standards provide coherent strategies for cross-border enforcement. The project will move beyond doctrinal analysis and also identify policy responses, including decisions to criminalise deepfakes, structures for civil liability, protocols for technological protection, and ethical principles, in order to determine the best method to trade off innovation and inventions with

the protections of human dignity and creative rights.

STATEMENT OF THE PROBLEM

The rise of artificial intelligence-induced deepfakes presents a serious legal and ethical problem in India, particularly where that technology is used to create explicit or pornographic content without consent. Deepfakes utilize machine-learning models to produce hyper-realistic images, audio, and video that oftentimes depict real people engaged in activities that they never participated in. Other than legitimate use of these technologies for commercial or creative purposes, which are also pervasive, their abuse is widespread in India where mainly women and public figures are the victims of nonconsensual explicit content. This form of abuse does reputational and psychological harm, and raises serious issues about whether India's existing intellectual property (IP) and allied legal regimes are sufficient. The Indian Copyright Act, 1957 defines copyright based on human authors and originality, which makes it poorly designed to deal with AI works with no identifiable human as creator. Moral rights, as identified in Section 57, protect against distortion or mutilation in or of an author's work, but in relation to its unauthorized use, do not apply to using someone's likeness in clear synthetic media. The law of publicity and personality rights, as recognized in case law (for example, ICC Development v. Arvee Enterprises), although recognized and cited, remains undeveloped and inconsistent, leaving victims of deepfake exploitation with inconsistent remedies. Furthermore, while the Information Technology Act, 2000 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 seek to regulate harmful online content, they are focused on intermediary liability and obscenity and do not account for intellectual property infringements that result from deepfakes. Moreover, with the absence of any clear statutory framework establishing ownership, infringement, or misuse of AI-generated media, there is ambiguity for victims, creators, and regulators in terms of action. In addition to this gap in regulations, jurisdictional issues hampered enforcement because explicit deepfakes would be shared on global platforms that are outside the effective territorial jurisdiction of Indian authorities.

Thus, the primary issue is the lag between technological advancement in the field of AI-generated media and the ineffectiveness of India's current IP and cyber laws in addressing the unauthorized creation and dissemination of explicit deepfakes, which threatens the rights and dignity of individuals while losing credibility in India's intellectual property regime as

technology continues to develop in the digital age.

RESEARCH QUESTIONS

1. Analysis of how Indian copyright and privacy legislations deal with ownership and accountability for explicit AI content, including deepfakes that utilise a person's likeness without permission.

2. Investigation of how individual legal protections in India extend to AI-generated deepfake content that contravenes rights to privacy, dignity, and reputation.

3. Identification of amendments needed in the laws surrounding intellectual property and privacy in India to regulate AI-enabled explicit materials and alleviate the harms of deepfakes.

RESEARCH OBJECTIVES

1. Examination of the copyright and intellectual property regimes applicable in India to the legal position of explicit and deepfake AI-generated content.

2. Determination of whether the privacy and data protection legal regime in India can effectively remedy the harms associated with deepfake and explicit AI-generated content.

3. Identification of gaps in the existing legal regime and recommendations for regulatory reform to legally regulate privacy and personality rights violations from AI-generated content.

RESEARCH METHODOLOGY

This research will be undertaken using a doctrinal methodology, primarily drawing on legal sources to examine the intersection of AI-generated works and intellectual property rights in India, with a specific focus on explicit content and deepfakes that infringe privacy laws. The research methodology will utilise qualitative and analytical methods, focusing on interpreting statutes, case law, and academic commentary, rather than collecting or analysing substantive empirical evidence.

Primary sources will include all statutory provisions of law, such as the Copyright Act of 1957, the Information Technology Act of 2000, the Indian Penal Code of 1860, and the Constitution of India, especially Article 21 on the right to privacy and dignity. Primary sources will include case-law from the Supreme Court and other High Courts to understand how Indian courts have developed case-law concerning copyright protection, privacy rights, and infringement of an individual's likeness. The secondary sources will include leading commentaries on Canadian law, Indian academic articles, international reports, and comparative analyses of foreign jurisdictions that address AI-generated works, explicit content, and deepfakes. The study will analyse whether the existing Indian legal frameworks can adequately address challenges posed by AI systems that generate explicit content and violate privacy. In this doctrinal study, the statutory provisions and case law will be interpreted to determine their relevance to the new challenges posed by AI-generated content. Transnational comparisons will be made to explore global approaches to AI regulation and to highlight possible lessons for India. Using this doctrinal method, the study will identify doctrinal gaps, analyze whether the current laws are adequate, and make suggestions for legal reform where appropriate to regulate AI-enabled explicit content and deepfakes, while also taking into account the need to protect intellectual property, privacy rights, and facilitate technology development.

Copyrightability and Legal Accountability of AI-Generated Explicit and Deepfake Content under Indian Intellectual Property Law

With sophisticated AI methods like deep learning and generative adversarial networks driving their creation, deepfakes have become among the most significant digital threats of our time. The capability of which to alter audio, video, and images with incredible realism, provoking significant privacy, defamation, misinformation, impersonation, and reputational harm issues. In India, the legal landscape, which relies primarily on the Information Technology Act, the Penal Code, and privacy jurisprudence, is piecemeal and reactive. None of it has been thought through continuously to address the knotty problems presented by deepfakes—undefined terms, difficulty tracking creators, ownership of likeness, and intermediaries and platforms lacking suitable liability models.[1] As technology becomes increasingly available, the dangers of exploitation have increased, specifically as it relates to political discourse, social trust, and individual dignity. Reflections on experiences from other jurisdictions suggest an increased need for regulation and the need to demonstrate that using existing legislation alone will not

[1] Kashish Gupta, The Future of Deepfakes: Need for Regulation, 5 NAT'l L.U. DELHI STUD. L.J. 130 (2023).

succeed. We need to establish broad, clear, and enforceable law as it relates to deepfakes, which should include clear definitions, liability, prompt restitution for victims, and also protect peoples rights and consent regarding their image. If we do not address this area through regulation, we risk eroding personal autonomy and social trust across all forms of digital media through the false production of visual images and events. Tort law, privacy rights, and intellectual property offer little to provide real protection, because they have the common challenges of the secret identity of a content creator, the ease of wider dissemination, and evidentiary challenges to support the harm. The gap in legal protections supports the need for narrowly crafted legal actions focused on harmful uses of deepfakes, while avoiding overly broad restraints on speech that might chill a respectful exchange of ideas. The challenging question remains, how to strike a balance to protect individuals from intrusive and harmful manipulation, and to respect the notions of free speech and political or artistic expression.[2] Third-party liability theories, including contributory infringement, vicarious liability, and inducement, have traditionally served to impose liability on an intermediary for the copyright infringement of others. However, the arrival of AI-generated works challenges the relationship between these theories and the idea of direct infringement. Despite the fact that a platform may host copyright infringing works, the platform does not actually create infringing works, but rather provides a technological framework for users to create and distribute their own content. This means that it is not easy to evaluate intent, knowledge, and control—all of which are relevant to liability under common law theories of third-party liability. Part of the challenge is finding the sweet spot between creating liabilities and facilitating innovation. Liability can be too strict and dissuade platforms from fostering technological innovation, and jeopardise or limit the right to free expression, or conversely, liability can be weak and essentially allow for mass abuse of copyright, with respect to deep fakes and sexually explicit materials. Current theories of liability were developed in top-down works of human creativity that cannot easily transition to a bottom-up algorithmic environment, particularly where responsibility is diluted between a platform's duties as platform owner, the user, and the AI system as creator of the works at issue.[3] There is sense to develop new liability pathways in ways that consider the potential implications of producing AI-generated works while providing robust mechanisms for copyright protection without necessarily choking off the development of new technologies.

[2] Shannon Reid, The Deepfake Dilemma: Reconciling Privacy and First Amendment Protections, 23 U. PA. J. CONST. L. 209 (January 2021).
[3] Sharon Choi, Assessing the Efficacy of Third-Party Liability Copyright Doctrines against Platforms That Host AI-Generated Content, 66 B.C. L. REV. 1087 (March 2025).

Deepfake technology presents multifaceted issues related to privacy, consent and copyright. With respect to privacy, unauthorized utilization of an individual's likeness, voice, or image in a manipulated video may grant rise to a significant violation of personal dignity and autonomy. The absence of consent, particularly when it comes to explicit video, materially aggravates the harm to the individual, subjecting him or her to additional reputational harm, harassment and emotional distress.[4]

With respect to copyright, deepfakes present the question of authorship and originality. The outputs are produced through an AI algorithm that employs an existing data set (usually without permission), and as a result, raises the question of whether the AI-generated deepfake is copyrightable or infringes copyright. Questions of ownership and liability also remain unaddressed, as typical copyright systems were not devised to regulate a piece of work to be autonomously produced. The intersectionality of these issues suggests a need for proactive legal regimes that please the creativity associated with deepfake technology while providing remedies for its misuse. The priorities of any legal regime must provide for protections based on consent, ensure there is clarity in copyright protection and copyright ownership and include liability for misuse of the technology to protect individual rights and property rights.[5]

Evaluating the Adequacy of India's Privacy and Data Protection Framework in Addressing Harms from AI-Generated Deepfake and Explicit Content

Deepfake technology presents significant threats to privacy due to its capacity to modify an individual's face, voice, or likeness without consent. These synthetic contents can be generated to create sexual content, defamatory content, or deceptive media that affect individual dignity, reputation, and mental health. Existing legal protections, including protections in the constitution and informational technology legislative protections, provide some benefits but are limited in scope, especially given the speed and anonymity which such material can flow through social media. The regulation of deepfakes raises ethical and constitutional challenges as well. Although there is a need to protect people's rights to their digital likenesses, restrictions that go too far could violate people's ability to express themselves. Thus, a thoughtful legal and policy response must balance protecting personal rights with protecting core freedoms. Possible proposals to address these dilemmas include considering digital likenesses a form of

[4] Intersection of Generative Artificial Intelligence, *J. Sci. & Tech. Pol'y Mgmt.* 17, no. 1, 118
[5] Santosh Kumar, *Legal Implications of Deepfake Technology: Privacy, Consent, and Copyright,* (2021)

personal property under intellectual property law, mandating that all AI-generated content be labeled as such, and increasing digital platform accountability to detect and take down harmful deepfakes.[6] The issue is compounded by the lack of specific statutory recognition of deepfakes, and as a result, the victim is put in a precarious position with few recourses. Technological countermeasures and interventions, such as detection algorithms, authentication tools, and watermarking, are being developed to combat misuse; however, they are also limited in their ability to keep pace with fast-moving generative technologies. Overall, an effective response will require a hybrid approach that brings together stronger legal protections and strong technological protections that address accountability and prevention in response to deepfake generated privacy violations. In India, the regulatory approaches to deepfake technology are currently both inconsistent and underdeveloped. While the constitutional right to privacy under Article 21, as well as certain provisions of the Information Technology Act, serve as a broad framework, protection is not specific to the challenges of AI-produced antisocial and harmful manipulation. Existing data protection laws including the proposed Digital Personal Data Protection Act focus on consent and protection of data but do not specifically address harms from non-consensual synthetic content.[7]

The lack of specific statutory recognition of deepfakes creates a vacuum in accountability, liability, and protection for victims. The existing frameworks explicitly struggle to regulate the speed, the scale, and the cross-national flow of manipulated media. Enforcement will remain reactive rather than proactive, without a clear legislative intent to protect.

India has made considerable progress in privacy and data protection law, particularly following the important Supreme Court decision that recognised the right to privacy as a constitutional right under Articles 14, 19, and 21. Previous regulations, such as the 2011 IT Rules on sensitive personal data, provided structure, but the Digital Personal Data Protection Act, 2023 marks a more comprehensive view of personal data protection in the rapidly changing digital landscape. Despite progress in privacy and data protection laws, several gaps remain. Specifically, current regulation does not contain timeframes for data breach notifications, nor does it provide a framework for cross-boarder transfers, potentially putting personal data at risk. Furthermore, there remains concern about the proliferation of governmental monitoring and the balancing of

[6] Aranya Nath & Sreelakshmi B., Deepfakes on Copyright Law - Inadequacy of Present Laws in Determining the Real Issues, 15 INDIAN J.L. & JUST. 285 (March 2024).
[7] Manish Nandal, *Mitigating Deepfake Threats to Privacy: Legal Frameworks and Technological Frameworks* (2022).

state interests with personal privacy. Comparison with a broader privacy framework, including elements of the EU's GDPR, also reveals alignment with international standards and gaps that offer opportunities for legal reform. To bolster data protection in India, steps should include establishing clear breach notification timelines, stronger regulations governing cross-border data flows, greater transparency in government data processing, and a public awareness campaign. It is important to address these concerns to establish a dynamic, responsive legal regime that protects citizens' privacy rights amid ever-increasing technological advancements.[8]

The legal framework in India regarding data protection has undergone significant changes, with privacy established as a fundamental right under the Constitution. In the past, in M.P. Sharma v. Satish Chandra and Kharak Singh v. State of U.P., the Supreme Court had dismissed the idea of privacy as a fundamental right. However, in 2017, a new Supreme Court ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India, established, for the first time, that privacy is an inherent part of the right to life and personal liberty in Article 21, thereby laying the constitutional groundwork for comprehensive data protection legislation in India. As digital technologies and personal data become more widespread, the need for effective laws to protect data will grow to mitigate the risk of misuse and to protect individuals' autonomy, safety, dignity, and identity. In terms of legal frameworks, the earliest visible examples, the 2011 IT Rules (on sensitive personal data) provided very limited protections and did not provide for enforcement. The Personal Data Protection Bill of 2018 attempted to build a comprehensive legal framework but was stymied due to data localisation and exemptions for government use, all of which significantly undercut its effectiveness. The passage of the Digital Personal Data Protection Act (DPDPA) in 2023 was a larger step forward in establishing a formal legal structure to protect digital personal data while also defining the role and responsibilities of those processing that data and establishing a Data Protection Board of India to hear grievances. The DPDPA bolsters privacy by giving individuals the rights to access, amend, and delete their data, while also requiring organisations processing personal data to be transparent in their practices, limit the purposes for which they use data, and minimise the amount of data they collect. There are still concerns about certain aspects of the DPDPA that could undermine its effectiveness in protecting privacy rights. Strengthening the independence of the Data Protection Board, promoting organisational accountability and transparency, enhancing enforcement mechanisms, and raising public awareness are all essential components to ensure

[8] Yashraj Bais, Privacy and Data Protection in India: An Analysis, 4 INT'l J.L. MGMT. & HUMAN. 1793 (2021).

that the DPDPA is effective.[9]

In conclusion, India's data protection framework is evolving into a more comprehensive legal framework that strives to align legislation with the constitutional right to privacy. Although there will always be evolving challenges when it comes to safeguarding privacy rights, the law will need to continue evolving reformatively and enforced consistently, to respond to the growing challenges of the digital age.

Legal Reforms and Regulatory Gaps to Address AI-Generated Content's Violations of Privacy and Personality Rights

The rapid growth of artificial intelligence and digital technologies has created serious problems for intellectual property law. Traditional lines of authorship and ownership have become more hazy due to the proliferation of digital content on the internet and AI systems' capacity to produce original works. Current legal frameworks, which were largely created for physical and human-made works, find it difficult to handle problems like content modification, widespread digital distribution, and illegal reproduction. The situation calls for comprehensive reforms that adapt intellectual property laws to the realities of modern technology, such as updating legal definitions to include AI-generated works, strengthening mechanisms to prevent piracy, and ensuring effective protection of creators' rights. These developments have revealed gaps in enforcement mechanisms and legal definitions, making it difficult to hold infringers accountable or to clearly define what constitutes infringement in the digital and AI context. Eliminating these gaps will allow the law to better protect innovation and creativity while maintaining a balance between public access and the rights of content creators in a technologically advanced environment.[10] Generative artificial intelligence has changed the game in content creation, enabling machines to generate text, images, music, and other creative works with very little human effort. While this has opened the door to growth and productivity, there are a number of ethical questions and legal concerns involved as well. One of the most salient ethical questions concerns authorship and originality; as AI-generated content becomes available, it blurs the line between humankind's creative activity and that produced by a machine, and raises questions about the author's rights to ownership and credit. Questions of

[9] Khushi Pradeep Rinwa, Understanding India's New Data Protection Laws and Their Influence on the Constitutional Right to Privacy, 6 INT'l J.L. MGMT. & HUMAN. 184 (2023).
[10] Pratyush Prakarsh , Tarun Sharma, Ujjwal Raj & Kriti Nand, Intellectual Property Law in the Age of Digital Piracy and Artificial Intelligence, 7 INT'l J.L. MGMT. & HUMAN. 1566 (2024).

responsibility emerge as well. If an AI engine produces harmful or biased or infringing content, we do not know whether the developer, the user or the system itself is responsible.[11]

From a legal perspective, intellectual property law is ill-equipped to address the sticky issue of autonomous human-machine creations, and there are gaps in determining copyrightability and ownership of copyright materials. There are even questions about using data sets to train the AI; following engagement with generative AI, data sets could include copyrighted content, raising questions of "fair use" or infringement. Furthermore, the potential misuse of generative AI could infringe on privacy or personality rights via the creation of deepfakes, misinformation, or other explicit content, with cascading impacts on trust in the broader public domain. Resolving the issues mentioned requires a balanced approach that encourages innovation while also respecting our accountability and rights. Ethical frameworks should prioritise transparency, fairness, and respect for human creativity; legal systems, in turn, should develop clear definitions, update regulations, and strengthen enforcement mechanisms. Together, this is important to effectively address the risks of generative AI in content creation, while appropriating societal values to technological developments.[12] To remedy these gaps, stakeholders and policymakers have increasingly advocated for stronger recognition and legal protections of personality rights, which give a person enforceable control over the commercial and personal uses of his or her voice, likeness, and image. In conjunction, the data protection regime needs to expand its remit to include biometric and identity-based information as personal information, so that any unauthorised manipulation constitutes a breach of privacy. In addition to reforming the legal framework, technological measures such as watermarking, tracking the provenance of information, and authenticating content can have a meaningful impact on detangling and tracing synthetic materials.[13] Yet, no single entity can ultimately manage the risks on its own. It becomes imperative to create the social good that compiles responsibility across public, government, technology companies, digital platforms, and an informed public that recognises manipulated media, raises awareness, and improves digital literacy.

[11] Antarjyami Mahala & Bhavin Chauhan, AI-Generated Innovations: Developing Intellectual Property (IP) Protection Framework for the Digital Age, 6 *Int'l Cybersecurity L. Rev.* 155 (2025).
[12] Yaso Hang Rai et al., *Ethical Concerns and Legal Implications of Generative AI in Content Creation* 2(1) 95 (2025).
[13] Shweta Deepak Sharma & Simran Gianchandani, Intellectual Property Rights and Artificial Intelligence: Need for Legal Framework, in One Day Multidisciplinary International Conference 8 (Ajanta Prakashan 2024).

Deepfakes pose more than a mere technological issue; they challenge longstanding assumptions about authenticity, identity, and trust in digital interfaces. Only a regulatory remedy that integrates the legal, technical, and social awareness and context in safeguarding privacy and personhood in a time when AI increasingly blurs the line between existence and artificial (fabricated) personhood.[14]

CONCLUSION AND SUGGESTIONS

The rise of AI-generated explicit content and deepfakes presents one of the biggest challenges for the Indian legal system. These technologies can alter people's images, voices, and likenesses without their consent, causing significant violations of privacy, dignity, and reputation. When such AI-generated content is sexual in nature, the situation is even worse because it is not just identity theft but results in psychological harm, harm to reputation, and social ostracisation. While existing laws like the Information Technology Act, 2000, and/or provisions of the Indian Penal Code, provide limited recourse against obscenity, defamation, and cyber harassment, they are not well-suited to address the challenges and changing landscape introduced by AI-generated fabrications. Similarly, intellectual property regimes are also stretched, given that intellectual property was designed around human authorship and does not specifically address offences involving misappropriation of identity or unauthorised use of personal data in training AI. The absence of clearly declared personality rights under Indian law also compounds the problem, leaving victims to pursue diffuse legal options. Simultaneously, enforcement mechanisms against deepfakes are retroactive, focusing on taking down harmful content only after it has been distributed, rather than offering protective measures. Without stronger legal and policy changes, India risks a future where people’s identities are turned into commodities, creativity is diminished, and trust in digital media is eradicated.

A holistic legal and policy approach is necessary that synthesizes more than one dimension. To begin, personality rights ought to be recognised by statute so that individuals would have the ability to assert an enforceable right to control their image, name, and voice. Along with that, the Information Technology Act and Indian Penal Code should be amended so that the creation and distribution of sexually explicit deepfakes are criminalised explicitly - thereby placing such crimes alongside existing legislation that criminalises voyeurism and cyberstalking. Civil

[14] Ayushi Singh, *Development of Personality Rights and Data Privacy Regulation of Deepfakes* (July 22, 2025) (unpublished manuscript), https://ssrn.com/abstract=5348028.

remedies should complement criminal remedies by increasing enforcement, allowing victims to obtain swift takedown, compensation, and injunctive relief. Furthermore, data protection regimes should expand to also cover bridging personal images and biometric data that were used to train AI to ensure scraping without consent was prohibited and developers are held accountable. The regulatory ecosystem must also use technology itself—such as requiring watermark, provenance, and content authenticity features in generative AI systems. Social media, social, and content-sharing platforms should use deepfake detection tools, take down content immediately, and accept heightened liability after repeat failures. Specialised redress options—like cyber tribunals or fast-track courts—will ensure timely determinations of complaints with relief issued on the spot. The petitioners who have access to these options will also need access to policy: public awareness campaigns and digital literacy training will help communities identify forms of manipulated content and limit its harmful circulation.

India must engage in international engagement to align regulations, collaborate on the development and use of detection technologies, and enhance enforcement against violators operating across borders. As a consequence, India needs to draw on multi-pronged strategies combining legal reform, technological safeguards, platform accountability, and public awareness. It is only through such a rights-sensitive, forward-looking framework that India can meaningfully respond to the challenge posed by explicit AI-generated content and deepfakes in a way that furthers the development of artificial intelligence in a manner that is in tune with constitutional values of dignity, privacy, and autonomy.

ANNOTED BIBLIOGRAPHY

1. Sharma, S, 2024. Redefining Liability; Intellectual Property Challenges in the age of AI, 2 LAWFOYER INT'l J. DOCTRINAL LEGAL RSCH. 316 (2024). https://heinonline-org-christuniversity.knimbus.com/HOL/P?h=hein.journals/lwfyrinl2&i=2542

Annotation – This article by Sharma provides a thorough examination of how India's conventional intellectual property (IP) laws—specifically those pertaining to authorship, ownership, and liability—are being disrupted by the quick development of artificial intelligence (AI). This work's industry-specific focus is one of its strongest points; it offers a well-founded, jurisdiction-specific critique that strikes a balance between doctrinal analysis and real-world applications. Comprehensive scholarship is demonstrated by Sharma's policy proposals, which include establishing new IP categories, revising authorship standards, implementing transparency measures for AI systems, and proposing enforcement measures targeting AI. However, the research mostly relies on theoretical debate and lacks empirical data and case-study analysis (e.g., jurisprudential outcomes). Additionally, there is no interaction with international IP regimes beyond passing mentions, which results in a lack of comparative analysis. To evaluate how courts distribute culpability, Sharma specifically highlights the need for empirical research, particularly case-law tracking of AI-generated material or inventions. He also draws attention to the lack of a comparative legal analysis of AI-authorship models between India and other jurisdictions, such the US or the EU. Furthermore, the impact of AI-generated discoveries on small creators versus huge enterprises remains an uncharted field. To properly guide law reform, future research should examine these issues through stakeholder interviews and empirical legal studies. This annotation highlights the essence of Sharma’s article, examines its merits and shortcomings, sets it within the broader research landscape, and pinpoints apparent actionable gaps for further research.

2. Narang, A, 2024. Exploring the Intersection of AI and IPR in the Context of the Emerging Phenomenon of Deepfakes, Journal of Intellectual Property Rights Vol 30, January 2025, pp 59-64. https://or.niscpr.res.in/index.php/JIPR/article/view/9984

Annotation- Ashna Narang examines the connections between deepfakes—AI-generated synthetic media that alter a person's voice, appearance, or personality—and intellectual property rights (IPR), especially in light of Indian and international legal systems. The study

illustrates how deepfakes undermine conventional IPR notions like personality rights, rights of publicity, and copyright by utilising AI technology, particularly GANs. Narang describes how deepfakes have disrupted the media, entertainment, and political spheres, emphasising the need to strike a careful balance between innovation and abuse. The author discusses potential remedies such as increased IPR enforcement, transparency mandates, intermediaries' liability, and comparative analysis with international jurisdictions, while surveying the legal protections available in India, including personality rights recognised by case law and the limited applicability of copyright and trademark frameworks. The article's thorough examination of individual rights under Indian jurisprudence and its thorough conceptualisation of deepfakes within IPR discourse are its strongest points. Narang effectively ties important AI concepts, like as GANs, to legal domains that protect similarity. The study, however, does not provide statistical information or empirical case studies on the frequency and consequences of deepfake lawsuits. Additionally, addressing new regulatory frameworks (such watermarking requirements or AI-specific laws) and delving deeper into comparative observations from international experiences may have expanded the scope. Narang outlines a number of specific research needs, including: (a) empirical studies that measure legal assertions and resolution in cases of deepfake IPR infringement; (b) a systematic assessment of how intermediaries, such as platforms, apply current IPR and content takedown regulations; (c) comparative legal scholarship that looks at jurisdictions with legislative models specific to deepfakes; and (d) an evaluation of technological countermeasures, such as watermarking and deepfake detection tools, in conjunction with IPR frameworks. To guide both legislative changes and policy responses, these topics warrant in-depth research. The criteria for a thorough annotated bibliography entry are met by this annotation, which combines a precise summary, critical review, academic linkage, and a keen identification of actionable research gaps.

3. Mohammad, S. Balancing the Risks and Rewards of Deepfake and Synthetic Media Technology: A Regulatory Framework for Emerging Economies, https://ieeexplore.ieee.org/abstract/document/10777194?casa_token=oPRAz09aZiEAAAAA:ze2vQZEnYX4dtamkX1lG_TXvC3NunH5qRzovATU-F7O9VY4vlefqJaGJ68akoEVDm08a8soJXjG3lg

Annotation- The simultaneous properties of deepfake and synthetic media technologies—which have both creative uses and significant risks—will be examined in this study, especially in light of rising economies. The research initiative examines the technological, ethical, legal,

and sociopolitical implications of AI-driven synthetic media tools, such as generative adversarial networks (GANs). On the one hand, these advancements have valid applications in fields including marketing, accessibility, education, and entertainment. However, they also provide serious risks, including copyright violations, political manipulation, identity theft, false information, and non-consensual pornography. The study's main goal is to create a regulatory framework that is suited to the difficulties encountered by emerging economies, where institutions do not have the resources or know-how to adequately handle AI-related damages and legal systems might still be keeping up with digital change. The framework would foster technological advancement while preserving individual rights and public confidence by seeking a balance between innovation and control.

4. Siva Vignesh, Nagarjun D.N. Legal Challenges of Artificial Intelligence in India's Cyber Law Framework: Examining Data Privacy and Algorithmic Accountability Via a Comparative Global Perspective. https://pdfs.semanticscholar.org/1f94/d69326a587ff32f1bc6e5bbd15b81651b9dd.pdf

In accordance with India's cyber law framework, the present research examines the legal and regulatory issues raised by artificial intelligence (AI), paying particular attention to data privacy and algorithmic accountability. India's current cyber regulations, largely based on the Information Technology Act, 2000, are under increasing pressure as AI technologies become more integrated into digital infrastructure across sectors such as healthcare and governance, as well as finance and surveillance systems. Employing a comparative global approach, the study will examine critically how prominent jurisdictions—including the US, Asia-Pacific nations, and the European Union (GDPR and AI Act)—are handling comparable issues. The objective is to identify best practices and make globally harmonised, context-sensitive reform recommendations for India's cyber law environment. By suggesting a thorough legal framework for India that encourages innovation while defending fundamental rights in the AI era, the report will add to the conversation about policy. Even though artificial intelligence (AI) is rapidly impacting industries such as banking, healthcare, security, and governance, India's current cyber law framework is still unable to address the specific legal issues raised by these technologies. The foundation of India's cyber legislation framework, the Information Technology Act of 2000, was enacted before the rise of artificial intelligence (AI) and does not specifically address issues such as algorithmic bias, automated decision-making, lack of transparency, and data-driven discrimination. Primarily in light of the upcoming Digital

Personal Data Protection Act (DPDPA), 2023, the majority of current Indian legal literature and policy discussions have either narrowly addressed data privacy or widely addressed digital data governance. Nevertheless, there is a dearth of scholarly and policy-focused research that incorporates algorithmic accountability into the larger framework of cyber law. Furthermore, there are few comparative studies that look at how other nations have incorporated AI regulation into their legal frameworks, such as the United States' sectoral regulatory approach or the European Union's AI Act, in the Indian context. It is more difficult to create a flexible, rights-based framework that can be successfully used in India's socio-legal context when comparative study is lacking.

5. Mohammed, I, and Sajith, S. Law in the Time of AI: A Critique of AI-Related Regulations, *27* Supremo Amicus [206] (2021). https://heinonline-org-christuniversity.knimbus.com/HOL/Page?public=true&handle=hein.journals/supami27&div=18&start_page=[206]&collection=journals&set_as_cursor=0&men_tab=srchresults

The legal frameworks governing artificial intelligence technology, both established and developing, are critically examined in this research. The authors examine the effectiveness, reach, and consequences of AI-related laws around the world, pointing out flaws and contradictions in the laws that are currently in place. They talk about how traditional legal concepts like accountability, transparency, and ethical standards are being challenged by the quick development of AI. The criticism highlights the necessity of flexible, progressive laws that strike a balance between innovation and public safety. Cross-jurisdictional legal disputes, the contradiction between regulation and technical advancement, and the importance of interdisciplinary cooperation in forming AI governance are some of the major themes. In order to guarantee responsible deployment and reduce harm, the study ends by arguing for more complex, adaptable legal frameworks that can develop with AI. The paper identifies a number of significant voids in the existing legal frameworks pertaining to artificial intelligence. The lack of a thorough and cohesive regulatory approach is one important gap. The fragmented and frequently jurisdiction- or sector-specific character of current legislation creates discrepancies and makes it challenging to handle the intrinsically global nature of AI technologies. The efficacy of regulatory initiatives is weakened by this fragmentation, which also demands for more uniform legal standards that are cross-border compatible. The essay also points out that ethical considerations including privacy, partiality, and justice are frequently ignored by

current legislation. Although a lot of laws concentrate on technical safety or compliance, they hardly ever incorporate interdisciplinary viewpoints that cover the moral and societal ramifications of artificial intelligence. This highlights the critical need for legal study that connects ethics, technology, and the law. Additionally, there is not enough attention paid to transparency and public involvement in AI governance. Most legal regimes lack safeguards that ensure AI decision-making procedures are transparent or that allow for significant public involvement, raising concerns about democratic accountability and social trust in AI systems. Finally, legal study has yet to adequately examine the wider socioeconomic effects of AI, such as inequality and job displacement. According to the paper, additional study is required to effectively control the revolutionary impacts of artificial intelligence on society by integrating these sociological factors into regulatory frameworks. All things considered, these gaps highlight the urgent need for multifaceted and flexible legal strategies that can successfully address the intricate problems presented by AI technologies.

6. Shweta Deepak Sharma, Simran Gianchandani, Intellectual Property Rights and Artificial Intelligence Need for Legal Framework. https://ajantaprakashan.in/pdf/International%20Conference_ISBN/English%20Part%20-%20III,%20Marathi%20&%20Hindi%20Part%20-%20I.pdf#page=8

Sharma and Gianchandani explore the evolving issues at the nexus of artificial intelligence (AI) and intellectual property rights (IPR) in this paper. They critically analyse how the intricacies brought forth by AI-generated innovations are outside the scope of traditional IPR frameworks, which were largely created for human inventors. The authors draw attention to problems like the uncertainty around authorship and ownership when AI systems generate original works on their own, as well as the effects of these advancements on copyright and patent laws. Through a thorough study, the article emphasises the need for a revised legal framework that protects the rights of human creators while allowing AI's involvement in innovation. In order to create an atmosphere where human creativity and AI developments may coexist and flourish, the authors support legislative changes that acknowledge AI's contributions without undermining the fundamental ideas of intellectual property rights. In the existing knowledge and regulation of intellectual property rights in the context of artificial intelligence, the paper highlights a number of important research gaps. The uncertainty around the ideas of authorship and ownership for AI-generated works is one significant gap. AI contradicts the fundamental tenet of traditional IPR rules, which presume human creators, and it is unclear from the law who is

entitled to what when AI operates on its own. This disparity raises issues about the equitable attribution and enforcement of intellectual property rights. Additionally, ethical and policy aspects are still poorly understood, especially when it comes to striking a balance between defending the rights of human creators and promoting AI progress. To create adaptive frameworks, multidisciplinary research that combines legal, technological, and ethical viewpoints is required. Lastly, there is a lack of research on effective enforcement strategies for intellectual property rights related to AI. It is yet unclear how to oversee, control, and uphold rights in the face of AI systems' constant learning and development, indicating a crucial subject for further study.

7. Weldon, Marcia Narine, Thomas, Gabrielle, and Skidmore, Lauren, Establishing a Future-Proof Framework for AI Regulation: Balancing Ethics, Transparency, and Innovation, https://heinonline-org-christuniversity.knimbus.com/HOL/P?h=hein.journals/transac25&i=266

The urgent need to create AI regulatory frameworks that balance important issues like ethics, transparency, and creativity while remaining robust to swift technology advancements is addressed in this paper. The authors contend that conventional regulatory strategies frequently fall behind AI developments because they are overly strict and reactive. They stress that ethical AI research, transparency in AI decision-making, and the creation of an environment free from needless restrictions are all important for effective regulation. The study examines several regulatory models, such as principle-based, adaptive, and participatory frameworks, emphasising both their possible advantages and disadvantages. To create adaptable yet robust AI governance frameworks that can evolve as AI technologies advance, the authors urge interdisciplinary collaboration among legislators, technologists, ethicists, and civil society. The paper highlights several research gaps that remain despite the in-depth examination. The absence of practical approaches to operationalise impersonal ethical ideas into legally binding norms is one significant gap. Even though ethics is a fundamental component of many frameworks, it remains very difficult to translate these principles into quantifiable, legally binding rules. The article also highlights the dearth of empirical research assessing the practical efficacy of principle-based or adaptive regulatory models for artificial intelligence. The majority of frameworks remain theoretical, and there is little information on how well they perform across industries and legal systems. Furthermore, there are significant gaps in international AI governance. Research on international cooperation models to regulate AI's

transboundary impacts is necessary, as the article emphasises the absence of coordinated global regulatory norms and enforcement mechanisms.

8. Jennifer S. Developing Legal Framework for Regulating Emotion AI, Bard, https://heinonline-org christuniversity.knimbus.com/HOL/Page?collection=journals&handle=hein.journals/jstl27&id=286&men_tab=srchresults

Jennifer S. Bard examines the recently emerged topic of emotion artificial intelligence (Emotion AI) in this article. She makes the case that this field needs its own legal framework, distinct from that of general AI or biometric data regulation. Emotion AI systems analyse human emotions based on physiological signs, vocal tones, and facial expressions. Bard highlights that the potential for Emotion AI to deceive people, violate emotional privacy, and propagate bias makes it a unique ethical and legal challenge, especially when applied in delicate settings like law enforcement, healthcare, education, and the workplace. The paper criticises existing legal frameworks for not sufficiently addressing the unique hazards posed by emotional inference technology, including the GDPR in the EU and the U.S. regulatory approach. Bard compares the need for more protections in emotion analysis to the permission requirements in healthcare, arguing that the subjective and individualised character of emotional data necessitates more stringent measures. She argues that, particularly as businesses increasingly integrate emotion detection into commercial and surveillance systems, depending just on generalised AI ethics concepts or current data protection legislation is insufficient. Although Bard offers a fundamental legal explanation of Emotion AI, there are still a number of significant research gaps. The lack of legal frameworks that explicitly classify emotional data as a distinct and delicate class is one of the main gaps. Emotion-based surveillance is generally unregulated because current privacy rules, such the GDPR or HIPAA, do not clearly distinguish emotional inference data from other personal or biometric information. This underappreciation highlights the need for more legal research to define and safeguard "emotional privacy" in a way that takes into account its behavioural and psychological ramifications. Bard urges the creation of thorough, Emotion AI-specific regulation that incorporates strong auditing procedures, required transparency, and informed consent procedures. Additionally, she supports limiting or banning the use of persuasive Emotion AI in situations where people might be most vulnerable, including clinical trials or job interviews. Her suggestions are in line with growing requests around the world for stricter regulation of

high-risk AI applications, such as those found in the EU AI Act and state-level privacy regulations in the United States.

9. Arbel, Yonathan, Tokson, Matthew, Lin, Albert. Systemic Regulation of Artificial Intelligence, https://heinonline-org-christuniversity.knimbus.com/HOL/P?h=hein.journals/arzjl56&i=564

Arbel, Tokson, and Lin contend in this determined and topical paper that the urgency of contemporary AI regulation necessitates a shift away from application-specific regulations—like those for automated decision-making or facial recognition—to thorough, system-level governance of AI as a general technological infrastructure. They note that policymakers are increasingly battling some of the most serious concerns posed by AI systems, ranging from societal-scale and existential threats to political manipulation and economic upheaval, and that legal scholarship has fallen behind technological advancements. The article's comprehensive perspective, which incorporates ideas from new research on complexity, resilience, and AI systems governance, is one of its strongest points. It provides tangible institutional pathways—from international treaties to national regulatory bodies—for putting systemic monitoring into practice and puts nebulous concerns about AI in a systematic taxonomy. It provides fundamental building blocks for future policy design as one of the first legal documents to genuinely address AI alignment and global existential risk. Arbel, Tokson, and Lin's paper Systemic Regulation of Artificial Intelligence offers a convincing argument for shifting AI regulation from disjointed, application-specific strategies to a more comprehensive, systems-based framework. Even Nevertheless, there are still a number of research gaps that need to be filled by future academics and decision-makers. The operationalisation of "systemic regulation" is one of the most noticeable gaps. Although the authors provide a theoretical framework, they do not go into depth about how such a regulatory framework would actually work in certain institutional and political contexts.

10. Tackling the Multifaceted Legal Dilemmas of Deep Fake Technology, 4.3 JCLJ (2024) 217, https://www-scconline-com-christuniversity.knimbus.com/Members/SearchResult.aspx

The article examines the increasing moral and legal dilemmas that deepfake technology presents, especially in light of Indian law. It critically looks at how current rules pertaining to intellectual property, permission, privacy, and defamation fail to handle the misuse of synthetic

media, including political manipulation, misinformation, and explicit content that is not consented to. The writers compare worldwide regulatory practices in the US, EU, and China while analysing loopholes in the Information Technology Act, 2000 and pertinent sections of the Indian Penal Code. As a comprehensive remedy, the study proposes a mix of legislative change, technological intervention, and digital literacy. It also emphasises the shortcomings of existing legal remedies in detecting, monitoring, and punishing the use of deep fakes. The authors provide a comprehensive approach to addressing the multifaceted concerns that deep fakes represent to individual rights and social confidence by addressing both the technological and legislative aspects of the issue. Although the report offers a solid basis for comprehending the legal quandaries presented by deepfake technology, there are still a number of important research gaps. The insufficiency of India's current legal system, which lacks clear clauses specifically addressing the production and distribution of artificial intelligence (AI)-generated synthetic media, is among the most urgent problems. Existing laws like the Indian Penal Code and the Information Technology Act of 2000 may provide some partial remedies, but they do not fully govern deepfakes, especially when it comes to situations involving impersonation, consent, or identity misuse. Additionally, there is uncertainty in both prosecution and victim redress because the Indian judiciary has not yet produced enough case law or precedent to direct the legal treatment of offences relating to deepfake. Furthermore, victim-centric treatments like accelerated removal processes, psychological assistance, or compensation frameworks—which are crucial in situations involving non-consensual explicit content or reputational harm—have not received enough attention. Despite being crucial in lowering societal susceptibility, the function of media literacy, digital education, and public awareness in halting the influence and spread of deep fakes is also not well understood. Finally, the duty of digital platforms to identify, flag, or delete synthetic information is mentioned, but more investigation is required to assess the suitability of the existing intermediary liability regulations and the moral standards set for Indian IT firms. When taken as a whole, these gaps highlight the necessity of interdisciplinary study and policy creation that connects human rights, technology, and law.