

Algorithms, Authorship, and Accountability IPR and the AI-generated Cyber-crime Dilemma

Ms. Priya Panwar

Student, Law

ABSTRACT

Generative artificial intelligence has transformed the production of text, images, music, software code, and multimedia. The legal dilemma is that copyright and cybercrime laws were primarily crafted around recognizable human makers, human decisions, and identifiable actions. Content produced by AI consequently creates two related questions: when intellectual property should attach to an AI-assisted or AI-generated work and who should be considered its author or owner; and who should be responsible when the same technology is used for deepfakes, impersonation, fraud, falsified evidence, or unlawful synthetic media. The study addresses these concerns primarily from the perspective of Indian law.

Keywords: Artificial Intelligence, Generative AI, Copyright, Authorship, Intellectual Property Rights, CyberCrime, Deepfakes, Synthetic Media, Accountability, Intermediary Liability.

1. Statement of the Research Issue

The primary research topic is the dissonance between traditional legal notions and AI-supported creation. Copyright law requires a discernible basis to determine the ownership of a protected work, while generative AI can create content without the traditional steps of human drafting or composition. Generative AI may create creative works without the traditional steps of human drafting or composition. If no AI-assisted works are AI-generated, the output is automatically granted copyright, the market may be flooded with protected material that lacks a clear human creative author. A clear, human creative writer is essential. If all works are AI-assisted, they are not protected; human artists who only use AI tools may still retain their rights. As a sophisticated tool, it may waive protection of authentic, original contributions. The second difficulty is about infringement.

Artificial intelligence systems might be trained or run on substantial quantities of existing works. A generated output can resemble previous work, repeat a protected expression, or mimic a distinctive style, potentially containing protected material. A distinctive style or contain protected material. The legal question is not always a simple matter to answer that it was "created by AI." Copyright infringement usually involves violations of rights that are protected by law. Acts of considerable reproductive communication or adaptation. The identification of the machine itself does not decide the matter. The cyber-crime dimension generates a comparable dilemma. Artificial intelligence can help make production easier. Fooling fake content. Existing offenses may apply to this conduct; however, investigations become more difficult when a suspect uses several accounts, foreign services, anonymous tools, or quickly removes content. The suspect uses several accounts, foreign services, anonymous tools, or quickly removed stuff.

Attribution, Preserving metadata and proof of intent and identity of the original developer may be problematic. The paper thus investigates how Indian law might assign rights and responsibility without generating either. Such a situation could result in either overprotection of machine outputs or a legal vacuum for hazardous synthetic content.

2. Objectives of the Research

The main purpose of this research is to analyze the ways in which Indian intellectual property law can address authorship and ownership of content created or generated with the help of AI. A second aim is to explore the association between content produced by AI and cybercrime offenses. This includes issues such as impersonation, cheating, privacy harms, unauthorized publication, and misleading synthetic content. The study also aims to discern between levels of human involvement in AI-assisted creativity. The study seeks to establish the conditions under which human creative input should warrant copyright protection. Another aim of the study is to investigate the evolving intermediary framework within information technology. Rules and the changing regulatory approach to synthetically generated information. The study, finally, presents a workable legal framework based on human creative input, transparency, provenance, suitable intermediary tasks, explicit duty allocation, and evidence retention.

3. Research Questions

Who should be considered the author/owner of AI-assisted and AI-generated material? under Indian copyright law? 2. Copyright Act, 1957, Section 2(d)(vi): Is it enough to include modern generative AI systems? 3. What is the line between human innovation using AI and content in Indian law? created with limited human artistic control? 4. Which existing cybercrime legislation can be invoked when AI is employed for impersonation, fraud, deepfakes, or other illegal activity? 5. How should intermediary liability and due diligence be applied when illicit synthetic content is uploaded on digital platforms? content is uploaded on digital platforms? 6. What legal protections can protect innovators and victims without unduly constraining application of generative AI?

4. Methodology of Research

RESEARCH This study adopts the doctrinal and analytical technique of research. The main legal materials regarded The main legal materials considered in this study include the Constitution of India, to the extent applicable, the Copyright Act of 1957, the Information Technology Act of 2000, the Bharatiya Nyaya Sanhita of 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021, along with official government material related to synthetically created content. Bharatiya Nyaya Sanhita, 2023 Information Technology (Intermediary Guidelines and Digital Media Ethics) Code) Rules, 2021 as modified and official government material relating to synthetically created data. Relevant material from WIPO and comparative copyright talks is used to comprehend worldwide models of AI-assisted authorship. The present study is qualitative.

This study does not attempt to quantify the number of AI-generated offenses or forecast the potential business impact of generative AI. The business impact of generative AI. Instead, it analyzes legal notions like authorship, originality, ownership, infringement, intent, attribution, and intermediary liability. The study also adopts a problem-based approach. The same AI technology can be used for both lawful creative activity and illicit conduct. The study makes a distinction between legal requirements and policy

recommendations. Where Indian law is not sufficientThe paper in particular recognizes the uncertainty rather than assuming that a proposed remedy is an actual legal rule.⁶ Content generated by AI: SIGNIFICANCE AND NATUREContent produced by AI is a broad term for text, photos, audio, video, code, or anything else that is generated fully or by means of an artificial intelligence system, partly, The system is particularly relevant because generative AI develops fresh material in response to a prompt or other input rather than just classifying or retrieving current data. But the term "AI-generated material" is too wide for legal examination.

There should be at least three cases. be divided 2. In the first, AI is a tool in a profoundly human act of creation. For example, an author can utilize an AI system to improve grammar, produce alternative sentences, and then independently rewrite the final article. In the second, the human provides precise instructions, chooses from several outputs, and amends large sections and arranges the end product. The third one is where the user provides a short instruction and receives the output. The output is generated without significant creative choices or transformations. This distinction is important because copyright protects expression and not an idea or an automated outcome. Similarly, WIPO debates regarding AI and copyright highlight the importance of human authorship and the scope of human creativity. control as the key issue. The U.S. Copyright Office has also made a distinction between AI as a tool of assistance and AI itself supplies the expressive elements in certain circumstances.

These comparison techniques are important for understanding the implications of AI in India. However, they are not directly determinative of Indian law. In cyber law, the kind of content produced by AI is also relevant. A manufactured image can be legitimate artistry. The content produced by AI can be classified as expressiveness, commercial use, satire, or an innocent experiment. This same technical capacity can also be used to create false evidence or impersonate individuals. fabricate evidence or impersonate an individual. The technologies used to create content exclusively determine its legal nature. The technologies used to manufacture it exclusively determine the legal nature of the content. Context, goal, consent, harm, and the appropriate law The concepts of right and offense remain important.

5. Copyright and AI-Generated Works Under the Indian Law



AI-generated works and the copyright question

The main legislation governing copyright protection in India is the Copyright Act, 1957. Section 13 identifies types of works in which copyright subsists, subject to the statutory conditions. Section 14 defines copyright as a series of exclusive rights in relation to distinct categories of works. Section 17. The first owner is generally the author, subject to legislative exceptions. The most relevant provision for this present topic is Section 2(d)(vi). It states that for a computer-generated literary, theatrical, musical, or creative production, “the person by whom the arrangements necessary to the creation of the work are undertaken” is considered the author. computer-generated literary, theatrical, musical, or creative production, “the person by whom the arrangements necessary to the creation of the work” is considered the author. This clause adopts the laws of India, uncommon compared to systems that strictly require human authorship.

It gives a statutory pathway for determining the creator of computer-generated works. The problem is that the phrase “necessary arrangements” was created for a previous technology. A human programmer or operator working in the normal manner would have computer-generated output configurations were easier to perceive. Today’s generative ecosystem includes model creators, data set providers, platform operators, prompt authors, users, editors, and occasionally several software suites. model creators, data set providers, platform operators, prompt authors, users, editors, and occasionally several software suites. It is therefore not always evident which person’s plans will decide the legal outcome. For instance, let us say a person creates a comprehensive prompt, generates twenty pictures, throws away nineteen, compiles. Manually alter the selected image and produce a final illustration from the features of three output images.

The user has since used a tremendous deal of creative judgment. The justification for legally recognizing the contribution of the user is stronger than where someone just types “create a landscape” and uploads the first automatic result. Section 2(d)(vi) should not, therefore, be regarded as automatically providing the same level of protection to all output generated by a generative model. The statutory provision indicates a potential author; however, issues of Originality, breadth of protection, and infringement still exist. A careful interpretation should consider what human contribution actually occurred, and whether the finished product contains protectable expression attributable to that contribution. This approach also avoids the issue of considering the AI system as a legal author per se. An AI model is not legally individuality because it generates smart content.

Copyright ownership creates enforceable rights and duties, which must be assigned to a person or legal organization capable of executing them. duties, and those rights must be attached to a person or legal organization capable of executing them.

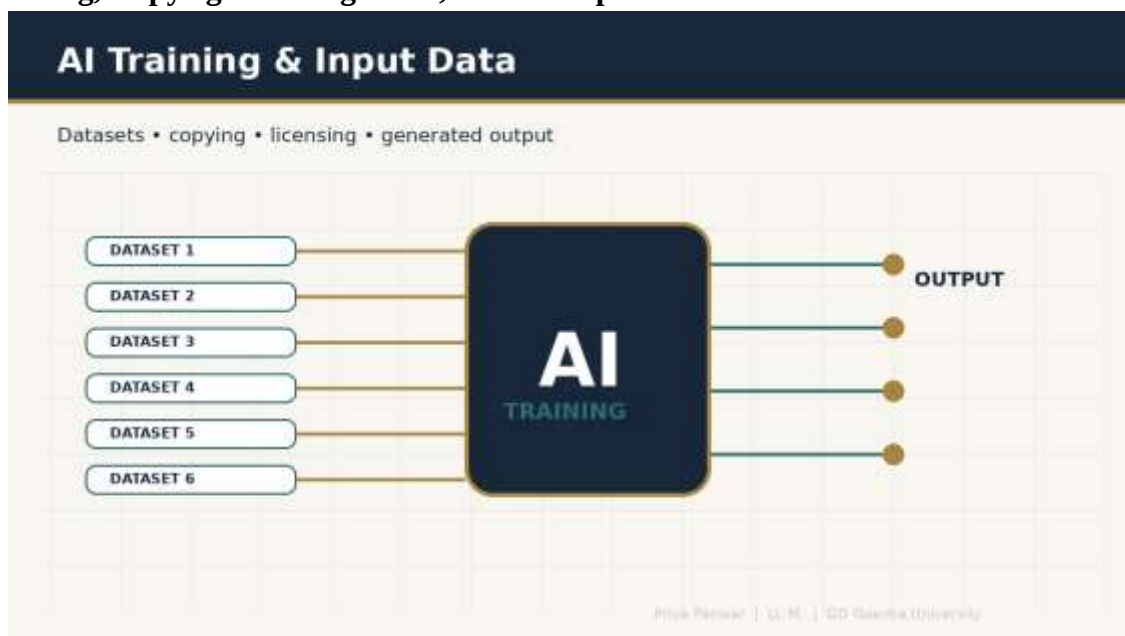
6. Authorship, Ownership, and the Criterion of Human Input

Authorship and ownership are not the same question. Authorship refers to the individual who wrote a work or is legally considered the author. legally considered the author of a work. Ownership asks who owns the copyright, and this might be the author or another individual under statutory laws or under contractual rules. Both questions can emerge in an AI-assisted environment. A relevant Indian approach would be to judge human effort in four practical terms. First, the nature of the instructions needs to be evaluated. A thorough instruction defining the composition, structure, Characters, order, or other expressive choices can demonstrate more human engagement than a basic request. Second, the choice should be considered. If the user reviews a number of outputs and picks out certain elements that selection might be part of the human contribution because of creative choices.

Third, alteration things.” Human rewriting, drawing, editing, arranging, or post-production can create protectable expression. Even when there was an initial starting point in AI, the final form should be reviewed. Fourth, the control of the final form should be reviewed. The “The stronger the authorship claim, the more meaningful control an individual has on expressive decisions. It should not be turned into a mechanical numerical test. Copyright law should not force someone to count the number of prompts or minutes spent editing. The question is, did the human really add original expressive options. The proposed approach can generate three generic classes. Category One: human-authored, AI-assisted work. Copyright should normally be treated in the same way as other human-made works, with oriented to human contribution. Category Two refers to mixed or collaborative creations in which AI contributes a significant amount of material, but the human is responsible for important selection, arrangement, and customization. much material, but the human does important selection, arrangement, and customization.

Protection can subsist in the human-authored portions and the final arrangement to the extent authorized by normal copyright principles. Category Three is an AI output that is minimally controlled. Where expressive choices are actually made by the machine, and human input is limited to a generic command, the case for broad copyright protection is significantly weaker. The machine makes expressive choices, while the human input is limited to a general command. This situation makes the case for broad copyright protection weaker. Protection is substantially poorer. This classification also minimizes the temptation to make false claims of authorship. A person should not become the author just by providing a prompt if the individual has no major creative input in the last expression.

7. AI Training, Copyright Infringement, and the Input Problem



AI training, input data and the infringement question

This issue is merely one aspect of the discussion around AI copyright. The other side focuses on the materials used to construct or educate artificial intelligence systems. build or educate artificial intelligence systems. Generative models are trained on very large datasets of text, photos, books, music, code, and other content. Where such material is copyrighted, questions/issues relating to copying, storage, extraction, licensing, and usage of the final model. The legal issue cannot be reduced to the

statement that training is either automatically permissible or automatically infringe. nature of the actual behavior, legislative exception, permission, contractual conditions, and Copying is to be looked at. Indian copyright law does have certain exceptions and limitations; however, it does not comprise one broad provision built expressly for generative AI training. It is necessary to distinguish between the input and the output.

A model may be trained on millions of works, yet it can generate output that is not significantly similar to any specific protected work. Generate output that is not significantly similar to any particular protected work. In contrast, a system can reproduce parts of a protected work that are identifiable. The examination of the law must consequently take into account the actual acts. This uncertainty affects the performance of the work and the interests involved. That uncertainty has commercial implications. "Creators may want to control or be compensated when their work is used for training." are used for training. Developers of AI may argue that wide availability of data is vital for the advancement of technology. development. Better licensing infrastructure and transparent records of datasets may be needed for a balanced framework. The new WIPO work on generative AI discusses copyright in training data, output protection, and the need for contractual systems for rights management, as well as explicit norms whenever legally and practically feasible. specific kinds of training utilized. In a similar vein, new WIPO work on generative AI discusses copyright in training data, output protection, and management of rights as related issues.

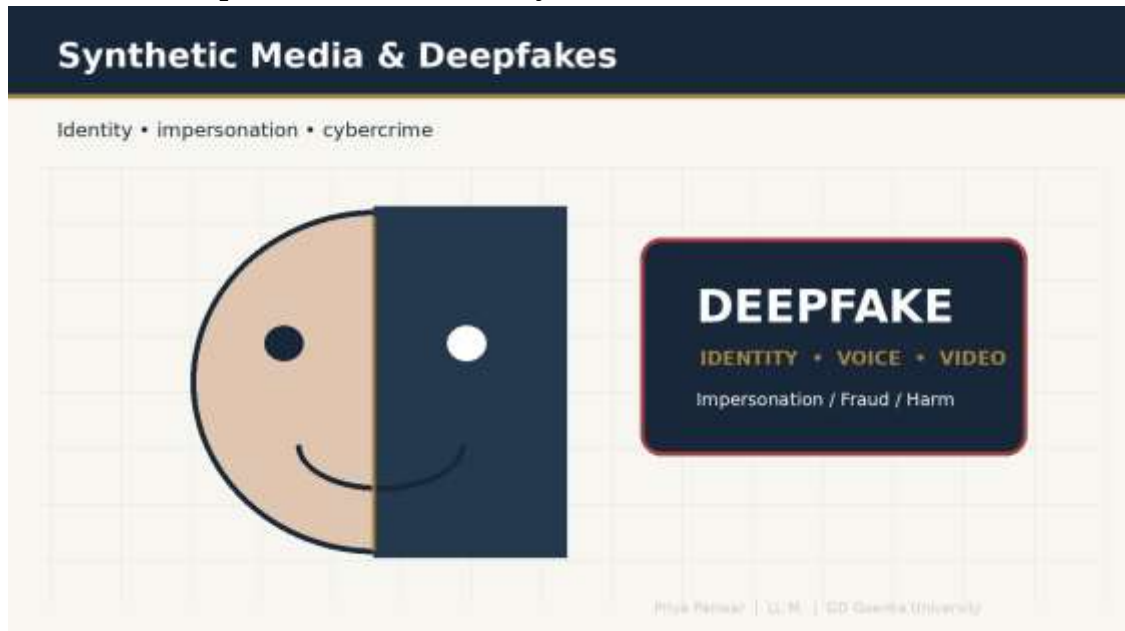
The worldwide debate consequently reinforces the argument that India should adopt clearer regulations instead of trying to solve every AI issue with one large ban. Rather than trying to solve every AI argument with one large ban, adopt clearer regulations.¹⁰ Content Created by AI & Cybercrimes Cybercrime's concern is the use of AI to carry out or assist in an illegal act. The technology itself is not always a crime. An AI image generator could be used by a person for academic purposes, such as creating visual aids for research, or for legitimate entertainment, such as generating artwork or graphics. A person could use an AI image generator for legitimate entertainment voice synthesis or drafting. 3. The project is an AI writing tool that addresses liability incurred by the user. the conduct, the injury, and the applicable legislation. One of the main areas is impersonation.

A synthetic voice or synthetic video might make it seem like one person has a voice or video that is not their own. This could lead to a situation where a person appears to communicate something they never actually said. Exploiting such technology to deceive a victim may invoke existing criminal laws. Provisions relating to cheating or personation may be applicable. Section 319 of the Bharatiya Nyaya Sanhita (2023) specifies cheating by personification and prescribes penalties for the offense. nCitenturn1search47n The Information Technology Act also contains relevant provisions on computer-related offenses. misuse of identity and illegal electronic publishing. Depending on the facts, provisions regarding identity theft, cheating by personification employing a computer resource, and sexually explicit or profane electronic material may be relevant.

The precise provision should be decided on the basis of the conduct, not just because AI was used. Artificial intelligence can help make fraud more believable. A criminal may synthesize a voice using personal information received from an outside source. received from an outside source and then called a victim claiming to be a family member, employee or official. The legal issue is the fraudulent activity, AI being the tool employed to make the deception more realistic. Deepfakes offer another concern in that they might harm reputation and public trust even before the Victims can prove who did this to them. Thousands of people can copy and repost a fake video. The first originator, the uploader,

and later the distributors could have varying levels of knowledge and intentions. A sensible legal system should therefore distinguish between deliberate invention and knowing publishing, reckless magnification and harmless redistribution.

8. Synthetic Media, Deepfakes, and the Liability of Intermediaries



Synthetic media, deepfakes and cybercrime risks

Indian intermediary regulation has been increasingly cognizant of the particular concerns posed by synthetic media. The phrase “Deepfakes and other synthetically generated” appears in an explanatory note by MeitY regarding proposed modifications for 2025. This information could result in disinformation, privacy harms, reputational loss, and electoral manipulation, and scam schemes. Then the regulatory framework moved further. The announcement in Feb 2026 revised the IT rules. The announcement also imposed additional obligations on significant social media intermediaries regarding synthetically produced data. Under the notified framework, competent intermediaries are required to receive declarations from users regarding whether the information is generated synthetically. The competent intermediaries are responsible for receiving declarations from users regarding whether the information is generated synthetically and for deploying relevant technical techniques to verify this information, with clear labels indicating that the substance has been verified as synthetic. This development is important because it moves part of the legal reaction from punishing after harm to tasks of the preventive platform.

But platform accountability should be proportionate. Automatic detection is incomplete. A system may misclassify genuine content as synthetic, while sophisticated synthetic content could go undetected, leading to censorship or overreliance on automated mechanisms. Such misclassification can result in censorship or an overreliance on automated mechanisms. Improper removal matters. The most effective technique is a multi-layered model. Platforms should have clear reporting methods and respond within legally mandated deadlines, maintain relevant documentation when necessary, and offer clear notices to users. Use technical measures proportional to the danger. Provenance and tagging of high-risk synthetic media techniques may assist users in comprehending that the material is not a regular recording. At the same time, liability for a

planned unlawful act should normally rest primarily with the person who authored or deliberately published the damaging material. person who authored or deliberately published the damaging material. Intermediaries should not become universal. Insurers are protected from any fraudulent statements that users upload. Their liability shall depend upon the proper statutory standard of due diligence and the facts of the case.

9. Comparative Perspective



Comparative approaches to AI and intellectual property

Varied legal regimes have varied approaches to AI authorship. Comparative debates at WIPO demonstrate that the essential issue is the level of authoring and control exercised by humans. The United States has typically established a human authorship requirement and recognizes protection for contributions made by humans to AI-assisted works, while refusing to fully safeguard material generated entirely by machines. AI-assisted works and the refusal to safeguard completely machine-generated material. India is unique in that section 2(d)(vi) specifically addresses computer-generated works and acknowledges the author is responsible for making the necessary arrangements. The provision allows flexibility, however, but it adds uncertainty when used with newer generating systems. The United Kingdom has traditionally applied a computer-produced work rule under which the person who is making the author is deemed to have made the appropriate arrangements.

This is a useful comparative example, as it demonstrates that a legal system may deal with computer-generated works without conferring legal personhood to the machine itself. WIPO has also named India and the United Kingdom among governments that utilize such an "arrangement." necessary" basis. The comparative lesson is that India should not simply replicate the legal frameworks of other jurisdictions. India has its own legislative regime and constitutional background. The beneficial lesson is that you can obtain clarity via a functional test that identifies human responsibility without claiming that all AI outputs have the same degree of human imagination.

10. Suggested Legal Framework for India

India can overcome the current uncertainties by combining statutory interpretation, regulatory clarity, and procedural protection. First, Indian copyright practice should recognize a human contribution appraisal of AI-assisted works. Registration and enforcement actions may require disclosing substantial AI involvement of human authors, when appropriate, should be followed by the identification of the portions they authored. This would not mean that AI is not always a copyright killer. That would just make it simpler to see the human contribution. Second, There is a need for legislative or authoritative guidance to clarify section 2(d)(vi). arrangements, the phrase "Necessary" should be read in the context of generative AI. The law must differentiate between the creator of a general-purpose model, the user who prompts the model, and the individual who edits content in the resultant work. creator of a general-purpose model, the user who prompts the model, and the individual who edits content to the resultant work.

The developer should not instantly become the copyright owner of every output. This is because the tool was created by the developer. Third, a provenance framework should be supported for high-risk synthesis content. Technical tags, content credentials, metadata, and platform-level records can aid in establishing whether a piece of media has been synthetically generated. Such actions should be structured with safeguards since Metadata can be changed or removed. Fourth, cybercrime investigations should be directed toward attribution and purpose. 14. CRITICAL DISCUSSION The most compelling case for maintaining human authorship is because copyright is intended to encourage and preserve human creative activity. If machine outputs are automatically entitled to full copyright protection, the quantity of protected works could increase massively without a human creative contribution to match.

This may cause uncertainty for future authors and raise the cost of using developed content. The most compelling reason for increasing recognition of AI-generated works is pragmatic. Growing use of AI as part of the normal creative process. A strict criterion that denies protection wherever AI is present would discount the fact that technology may complement, not substitute, human ingenuity. Indian law can tolerate this middle position because Section 2(d)(vi) already uses the language of preparations needed for computer-generated art. The problem is to interpret the provision in a consistent way with creativity and the real input of the human person. On the cybercrime side, it is a similar balancing act. Synthetic media can be heavily regulated since they can enable fraud and impersonation to a level that was difficult to pull off earlier. But under criminal law it should be rooted in the time-honored principles of actus reus, mens rea, and proof.

A person shall not be criminally liable simply because the computer-generated image resembles a real person. There has to be a legal acknowledgment, wrong and adequate proof to tie the accused with it. The key policy choice should therefore be proportionality. High-risk uses such as fraud, intentional More robust protections are needed for impersonation and illicit synthetic media. Creative use should remain low-risk, relatively open. Instead of suspiciously observing the mere application of AI, the law should restrict hazardous behavior. 15. RESULTADO The paper finds that content produced by AI creates a real legal gap only if the categories in place are reconsidered as if all AI output were the same. The necessary tools are already available in Indian law, but their application to Modern generative AI has to be better interpreted. First, under section 2(d)(vi) of the Copyright Act, there is a legislative baseline for computer-generated works. But the present sense of "arrangements necessary" has to be explained.

Second, the human creative input must be at the heart of the copyright protection. Prompting, Choice, organization and editing may be part of such input, but a generic instruction followed by automatic Publishing should not immediately confer extensive authorship. Third, AI training presents distinct copyright issues regarding the usage of copyrighted input content. These Questions of ownership of outputs should not be conflated. Fourth, cyber-crime legislation in place could be invoked when AI is used to cheat, personify, unauthorized publishing or offenses in connection with it. The fact that AI was utilized does not in itself cause an offense, and there is no particular “deepfake offense,” but this does not indicate that detrimental conduct is outside the law. Fifthly, the roles of intermediaries are getting increasingly defined. The 2026 IT Rules revisions hint at a shift toward disclosure, technical verification, and labeling of synthetically generated information for important social media middlemen. Sixth, enforcement is only effective if there is evidence.

Prompt records, source files, upload logs, account information, metadata, and other digital recordings could be essential in determining authorship and criminal accountability. Finally, the optimum long-term answer is a layered structure of copyright principles, cybercrime law, platform due diligence, provenance regimes, and effective victim remedies. 16. Generative AI has established a new legal landscape where the boundary between human invention and the production of machines is no longer Indian law’s core challenge; it is to protect authentic human creativity and, at the same time, to prevent abuse and to leave space for technical growth. The Copyright Act 1957 already offers an important statutory foundation through its regulation of works generated by computers. Modern generative AI, however, requires a more thorough appraisal of human involvement, especially if a system makes most of the expressive decisions. The law should differentiate between AI as a creative tool with AI as its major mode of expression. Meaningful human selection, arrangement, and modification should stay relevant for copyright protection. The problem of cybercrime requires a new focus. When you utilize AI to impersonate, deceive, defraud, or disseminate unlawful synthetic content, liability should attach to the underlying wrongful behavior. 17. SHORT SUMMARY The key challenge this paper addresses is that AI is now capable of generating information that looks and sounds like it was made by a human. That raises two big legal problems. The first is intellectual property: if an AI generates an article, image, song, or video, who owns it? The second is about cybercrime—if AI develops a phony video, who is liable for the voice or image used for fraud or impersonation? Indian copyright law already includes a paragraph for computer-generated works.

Section 2(d)(vi) of the Copyright Act deals with the person who takes the arrangements for the author as creation. The problem is that current AI has many participants. The model may be designed by one firm and operated by another platform to be used by a third person. The You may also alter the output. So the law needs to look at the real human contribution. REFERENCES 1. Government of India. Copyright Act, 1957. The India Code. 2. The Information Technology Act, 2000, India Code, Government of India. 3. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, as revised. 4. The India Code Government of India Bharatiya Nyaya Sanhita, 2023. 5. Explanatory Note on Planned Ministry of Electronics & Information Technology modifications to the IT Rules, 2021, on synthetically created information, 22 October 2025. 6.

Notice of amendment of IT Rules by Ministry of Electronics and Information Technology, February 2026 on synthetic-created information, 2021. 7. World Intellectual Property Organization, Artificial Intelligence and Copyright. 8. World Intellectual Property Organization, Generative AI: Intellectual Property Considerations 2024, Property. 9. WIPO Conversation on Intellectual Property World

Intellectual Property Organization & Frontier Technologies, AI authoring and synthetic media, 2025.10. U.S. Copyright Office, Copyright and Artificial Intelligence: Part 2, Copyrightability, 2025. 11. Fritz, Johannes, "Authorship in Artificial Intelligence-assisted works," *Journal of Intellectual Property Law & Practice* (2025). 12. ANI Media Pvt. Ltd. v. OpenAI OpCo LLC, in the High Court of Delhi, Important orders and pleadings about generative AI and copyright, 2024-2026.21.

Content created by AI AND THE PROBLEM OF ORIGINALITY The first legal problem posed by generative artificial intelligence is the issue of originality. ©Copyright Generally, the law protects original expression, not an abstract idea, fact, or concept. AI-created material confuses this distinction, since the final output may be generated from a combination of a user's prompt, the model's learned parameters, automated processing, and material from its training data. A human user may have some control over the choice and direction, but the degree of human creative input can differ greatly from one example to another. Very little human creativity may be involved in a simple suggestion like "write a short poem about rain" in the last expression. Conversely, the user who develops a detailed concept, contributes characters, structure, research material, stylistic guidelines, and periodic revisions of the result can exercise far greater creative control. The legal issue is therefore not only whether AI was employed, but also how much human intellectual contribution can be seen in the final product. This subject is crucial for Indian copyright law because the Copyright Act, 1957, contains notions of originality and original literary, theatrical, musical, and artistic works developed before Creative AI became commonplace.

The statutory framework does not give a complete category made for autonomous generative systems. Courts and legislatures may consequently have to consider the real contribution of the human claimant, rather than treating all AI-assisted labor the same. A pragmatic approach would differentiate between AI-assisted creation and largely autonomous generation, where a human author makes significant creative decisions and exercises control over the expressive elements; copyright protection may be more easily justified. If the result is virtually entirely produced through automated generation with little human input, the claim of human authorship becomes significantly weaker. This differentiation could be a useful beginning point, without making them separate legal persons. an artificial intelligence system.

11. Who Owns the Content Created by AI?

Authorship is a different question than ownership. Even if a work is eligible for legal protection, the law requires decide who is entitled to exercise the applicable rights." In traditional creative production, authorship and first ownership are typically closely related, subject to employment, assignment, and other legislative provisions. AI-generated material breaks this relationship, as a number of actors may claim an interest: the person who entered the prompt, the developer of the AI model, the access provider, the employer, or the commissioning party, and perhaps the creators whose work was part of the training data set. The user may assert that the output was developed based on their input and that their creative support ownership decisions. The AI developer can depend on the terms of the contract that governs the service. A boss may have claims under employment agreements.

A commissioning agreement may transfer rights to a customer. And these possibilities indicate why technology alone cannot answer the question of ownership. Contractual arrangements regarding a copyright are already recognized under Indian law. Thus, parties employing Creative AI in professional environments should define ownership and permissible usage ahead of time. Contracts indicate whether AI-supported material is commercially exploitable, whether disclosure of AI use is necessary, who is

responsible for third-party infringement, and what occurs if an output is contested. However, contractual allocation cannot create copyright in content that does not satisfy the legislative obligations for protection. A contract can assign contractual rewards or contractual burdens/duties, but does not necessarily turn an otherwise unprotectable output into an original work.

This distinction should stay front and center when drafting generative AI-related agreements.

12. AI Training Data and Copyright Infringement

Generative artificial intelligence systems are trained on massive datasets. Those datasets might comprise books, articles, photos, artworks, music, software code, websites, and other protected content. The legal debate at several stages: collecting of works, copying for training, storage and processing, model development and output generation. Each level could present a distinct legal issue. The most challenging question is whether copying protected works for machine learning purposes is infringement or is subject to an applicable exception. The solution cannot be presumed only because the copying happens for technological or research reasons. Copyright law controls certain actions of replication and communication, except as otherwise provided by statute or by court decision. Fair dealing protections and certain legislative exceptions are included in Indian copyright law; however, these were not designed primarily for large-scale generative AI training.

Using existing exclusions for commercial use Machine learning applications may require rigorous judicial scrutiny. Factors like purpose of use, nature How much was copied, the market effect, and the precise legislative exception that applies may become crucial to the work's value based on the claim type. Another issue is the link between training and production. A model can learn statistical regularities from millions of works without replicating any one work in a recognizable form. And yet there might be times where an output substantially reproduces protected expression. The legal analysis needs to differentiate among abstract learning of patterns and identifiable reproduction of protected expression. Treating all AI outputs as infringement would be overly broad, while ignoring close reproduction would leave rights holders without an effective relief.

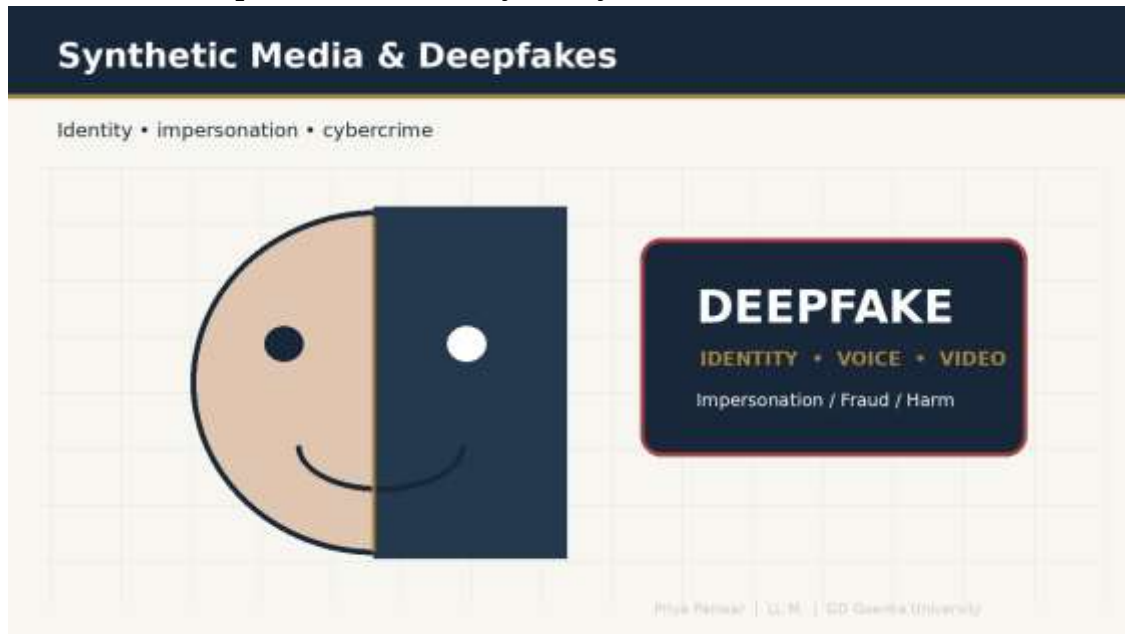
13. Imitation, Transformation, and Moral Rights of Style

Generative artificial intelligence is able to develop content that mimics the style of a renowned artist, writer, photographer, or movie maker. Copyright is normally protected. It is challenging to classify style itself as a copyright-protected subject, as copyright expression and not a broad creative technique or notion. A legal distinction must consequently be drawn between copying protected material and merely creating fresh expression that is inspired by a recognizable style. The problem is especially acute where an AI output reproduces identifiable features of a particular work. If a system produces an image that nearly replicates the composition, characteristics, and distinctive protected representation of an existing work, the problem is different than developing a creative image that just uses a same wide-art technique. Moral rights add a further layer.

Special rights of authors under the Copyright Act relating to distortion or modification of works in the circumstances to the prejudice of the author's reputation. Artificial intelligence systems can alter or remix existing works on a scale not imagined when many copyright doctrines were formed. Answer A system may also blend works in ways that strip context or establish an association that the original creator Never meant. Future conflicts may consequently need courts to balance economic rights and personality-

related interests. The legal solution should not grant authors a monopoly in an abstract way but yet safeguard recognizable expression, and genuine interests in attribution and integrity.

14. Synthetic Media, Deepfakes, and Liability for Cybercrimes

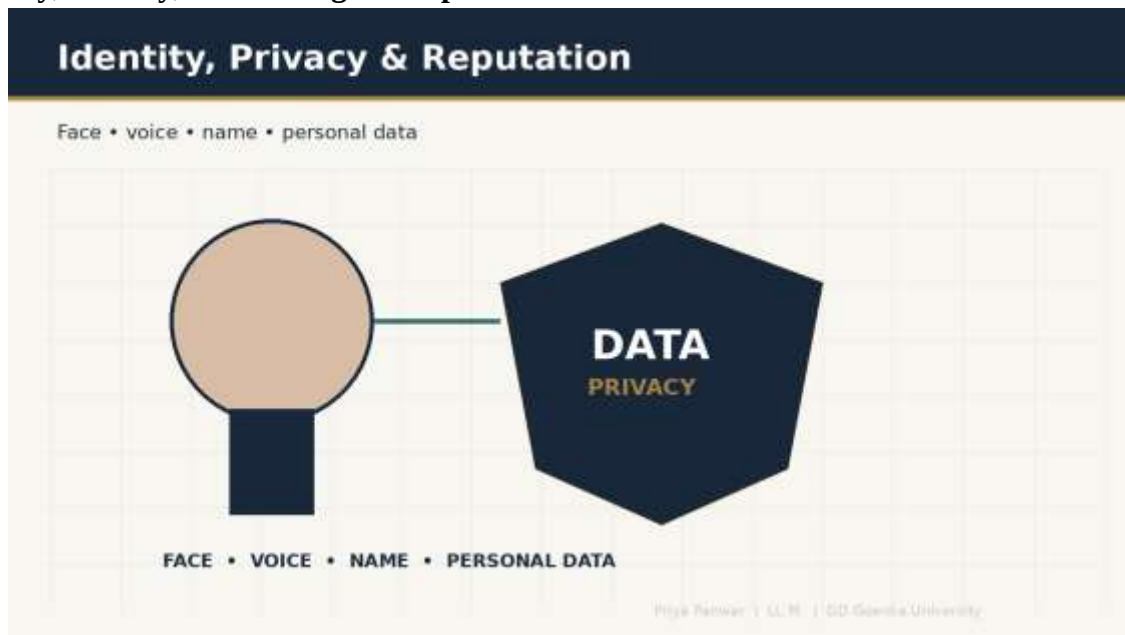


Synthetic media, deepfakes and cybercrime risks

AI-generated images, audio, and video establish a direct link to intellectual property law and cybercrime laws. A synthetic video might be benign entertainment, political satire, or an educational exercise. However, the same technology may also be used to impersonate someone, propagate false information, and conduct fraud. It can endanger a person or ruin reputation. The legal classification is thus very dependent on the goal, background, and effects of the act. Various legal options are available under Indian cyber law based on the facts of the case. The Information Technology Act, 2000, covers offenses connected to identity, privacy, computer resources, and electronically transmitted material. The Bharatiya Nyaya Sanhita, 2023, also provides for offenses that could be relevant in cases when synthesized media is used for cheating, impersonation, defamation, intimidation, or other illegal activities.

The specific offense focuses on the behavior, not the existence, of AI-generated stuff. Attribution is a huge challenge. A deepfake may be developed anonymously and uploaded through several accounts and quickly shared across platforms. Therefore, investigators may have to establish the source, account device information, ownership, metadata, payment records, and other digital proof. The probative value of digital content shall likewise be subject to the law applicable to electronic evidence. The legal reaction should also differentiate between creator, original uploader, middleman, and ordinary user who distributes modified material without their knowledge. Responsibility for crimes should generally be based on knowledge, intent, involvement, and the particular offense proved by the evidence. Automatic responsibility in criminal law for each individual who shares synthetic content would be excessive and could disincentivize legal discussion and the lawful expression of.

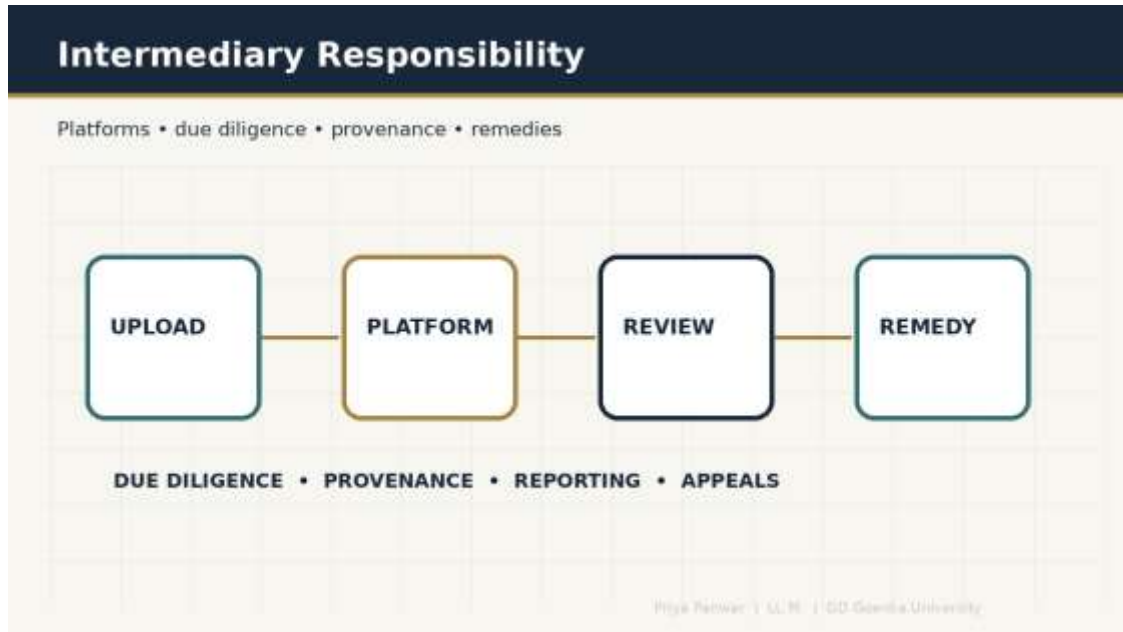
15. Identity, Privacy, and Damage to Reputation



Identity, privacy and reputation in synthetic media

Content created by AI can utilize a person's face, voice, name, or other recognizable features without agreement. This raises problems about copyright, privacy, and personality. A person in a photograph may be protected by the copyright of a person other than the represented subject, and the depicted individual's own legal rights may result from rights of privacy, dignity, reputation, or personality. These rights are not the same. Voice cloning presents a particularly difficult task. A person's voice could not fit easily into the usual copyright areas, but it can do considerable damage when unlawful synthetic use is made when listeners are led to believe that the guy said anything at all. The same is true of facial reconstruction and impersonation. The fundamental right of privacy under Article 21 is an important underpinning principle, especially where independence and personal identity are compromised. The Digital Personal Data Protection Act, 2023, can also be relevant in cases when personal data are processed within the scope of its regulatory framework. But privacy law, data protection law, copyright law, and criminal law deal with separate interests and should be implemented according to their unique needs. A good legal system has to allow fast remedies for clearly unlawful synthetic content, procedural precautions against false accusations. Platforms should have accessible reporting procedures, and victims should be able to know the rationale of a removal decision and contest an erroneous option.

16. Intermediary Liability and Platforms' Responsibility



Intermediary responsibility and platform safeguards

Online platforms are at the heart of the dissemination of content produced by AI. They do not form the content yourself, but their services enable instant and worldwide distribution. Indian intermediary legislation hence becomes relevant in case of uploading or sharing illegal synthesized content. The Information Technology Act, 2000, establishes a safe-harbor framework for intermediaries subject to the provisions of the Information Technology (Intermediaries Guidelines) Rules, 2011, and amendments thereto. statutory conditions. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) The Rules, 2021, further stipulate due diligence duties for intermediaries. The challenge in law is to implement these duties to content produced by AI without making platforms universal pre-publication censors. In 2021, platforms implemented technical and procedural controls, including content provenance, reporting systems, information, synthetic material labeling, repeat offender methods, and preservation of evidence for legitimate investigations. information, synthetic material labeling, repeat offender methods and preservation of evidence for legitimate investigation. . . .

At the same time, automatic detection is not fully reliable. false positives can be removed. This includes fair satire, parody, journalism, studies, and satire, parody, journalism, study, or artistic experimentation. So a tiered system is the stronger strategy. Illegal stuff should receive a faster response where the legal requirements are studied. The more unclear the material, the more it requires human or procedural review and an opportunity to confront. Transparency reports can also help clarify the level faster. complaints, removals and appeals are won.

17. Software Code Generated by AI and Software Copyright



AI-generated software code and copyright compliance

Generative AI is rapidly being utilized to build computer programs, scripts, and code. This produces a certain copyright issue as computer programs are protected as literary works under Indian copyright law, while the development process can incorporate enormous amounts of pre-existing open-source and proprietary code. The developer, using AI to produce software, can think that the code is totally original. But, The (a.b.x.c == b.b.x.c) { return 0; } if (a.b.x.c < b.b.x. c) { return -1; } return 1; This is more pertinent where the training material includes open-source software that is subject to the conditions of its license. Therefore, there is a possibility of copyright risk when the output was produced automatically. The problem is not open-source. Open-source licenses may be licensed. Itions about attribution, dissemination and modification.

If AI-generated code contains protected code covered by a certain license terms, the user may have contractual open-source duties. Therefore, organizations that use AI coding tools should have review procedures in place. Developers have to check code, check dependencies, keep records of material prompts where applicable and review licensing of commercial software with substantial AI-generated components prior to AI aid should not be a substitute for normal software compliance practice applicable,

18. Evidentiary Issues in Cyber Crimes in the Light of Artificial Intelligence



Digital evidence, attribution and preservation

AI-related disputes raise new evidential issues, because digital content can be created, modified, and swiftly redistributed. A screenshot doesn't tell you who produced a piece of synthetic content or when it was generated, whether it was later modified, or whether the accused actually uploaded it. Priya Panwar, LL.M. Research Paper | 13 Digital evidence may include server logs, device logs, account information, timestamps, metadata, payment details, IP information, and platform data. Investigators have to prove authenticity and a dependable chain of custody. Courts must also be aware of the possibility that seemingly legitimate digital information has itself acted. Another dimension is added by generative AI, because the detection techniques can produce probabilistic findings. An AI DETECTOR may provide the impression that the content looks manufactured, although such a conclusion should not be drawn automatically of evidence of authorship or criminal responsibility.

The evidential value of a technical report depends on its approach, reliability, and the facts of the case. Thus, confirmation is required for a solid legal strategy. Technical detection might be one piece of evidence among numerous rather than a substitute for proof of intention and activity. This is very essential in criminal procedures where the prosecution must meet the relevant standard of proof.

19. Regulatory Challenges for Indian Law

Indian law now addresses AI-generated harm by combining existing intellectual property, information technology, criminal, privacy, and contract principles. This strategy offers a number of legal options. Yet it also raises uncertainty, as no single regulation fully defines AI-generated content, authorship, ownership, synthetic impersonation, and model training liability. A future legislative framework must not involve superfluous redundancy. Instead, it could explain specific questions that are not answered by existing legislation. These may include the legal treatment of substantially autonomous output, disclosure obligations for high-risk synthetic material, provenance obligations in defined conditions, obligations of large platforms, and solutions for victims of unauthorized identity manipulation. And as far as practicable, regulation should be technology neutral.

A rule written for a certain model or technical technique may soon become outmoded. The focus should be on conduct and harm: unlawful reproduction, fraudulent impersonation, privacy infringement, fraud, harmful manipulation, and illegal distribution. At the same time, regulation should not kill legitimate innovation. AI is also utilized for education, accessibility, research, translation, software development, and creative experimentation. Overly sweeping regulations could interfere with lawful speech and technological innovation.

20. Comparative Perspective: United States, European Union, and British Isles



Comparative approaches to AI and intellectual property

India also has useful points of reference in comparative legal systems. The U.S. has adopted an approach to AI copyright questions through existing copyright doctrine, governmental guidance, and litigation, with a strong attention to human authorship. The Copyright Office of the United States has considered whether human creative contribution is enough to preserve AI-assisted material. The European Union has chosen a more extensive regulating approach with the EU Artificial Intelligence Act, which introduces requirements depending on the risk provided by artificial intelligence systems. It also features transparency obligations around specific types of AI-generated or altered content. Copyright and data-related duties interplay with the larger regulatory regime. The United Kingdom has previously discussed a law provision for computer-generated works, making a distinctive comparative question for works not produced by a traditional human author.

The system; The UK method shows that legislators can adopt special regulations for automated production, albeit the policy option is controversial. India has no need to follow any foreign model. Constitutional structure, copyright law, digital economy, and societal situations are different. Yet comparative experience is useful in detecting recurrent principles: human accountability, openness, proportionality, protection of intellectual rights, procedural protections, and targeted control over dangerous uses. Priya Panwar | L.L.M. Research Paper | 14

21. Proposed Legal Framework for India



A possible legal and institutional framework for India

balanced Indian framework should start with a classification of AI-generated material by degree of human engagement and the nature of the legal danger. Works aided by AI with some human ingenuity can be judged using existing criteria of copyright. “Mostly autonomous outputs could need different treatment as copyright protection and ownership are concerned. Second, the legislation should give more precise guidelines on AI training. Commercial developers need to keep clear records of the categories and lawful sources of training material, if possible. Licensing procedures, valid access, and reasonable exclusions can be addressed by legislation and policy rather than depending only on lawsuits. Third, high-risk synthetic media should be subject to suitable disclosure standards. Content that significantly impersonates a genuine person or develops a plausible false representation may necessitate disclosure or provenance information, subject to certain exceptions for news, parody, research, and other authorized uses. Fourth, victims should have access to remedies.

A person whose identity is abused by a deepfake should be able to request removal, retain evidence, and seek appropriate legal relief without having to go through an unnecessary difficult method. Enforcement should focus, finally, on actual harm and blame. Criminal sanctions ought to be limited to behavior that satisfies the criteria of an offense. Civil remedies, platform policies, and administrative measures can resolve lower-level disputes more equitably.³³ **CRITICAL COMMENT** The core problem in AI and intellectual property law is the difference between the speed of technology and legal categories. “Copyright law originated around human creativity, recognized works, and relatively steady modes of copying. Generative artificial intelligence can currently create vast amounts of text, images, audio, and code in seconds. The law therefore has to decide what portions of this process warrant protection and what produce liability. One extreme would give every product of AI extensive proprietary rights.

This could lead to excessive claims controlling content that has no human ingenuity and exposes lay consumers to overlapping rights. The contrary extreme would consider all AI-generated material to be legally unfettered. That could weaken incentives for humans, creators, and leave dangerous reproduction without appropriate remedy. A better approach is a differentiated framework. Human creative input must remain important to copyright authorship. A contract should be a tool for apportioning rights between

users, employers, and service vendors. Training disputes should be evaluated in relation to the specific acts of copying and relevant vendors' training in cybercrime should rely on the illegal act and the mental element required by the offense in question. Accountability should still be tied to identifiable human and institutional actors. Artificial intelligence systems cannot if the law requires, meaningfully substitute the legal obligation of developers, deployers, users, or platforms. Duties to be imposed on them.

It is so to be expected that the aim should be to control the people and organizations that can make decisions, rather than as a legal agent independent of the algorithm.³⁴ **STUDY RESULTS** The study indicates that AI-produced material raises overlapping concerns of copyright, authorship, ownership, privacy, data protection, intermediary responsibility, and cybercrime. These problems can't be remedied in a single legal principle. The study also suggests that the human creative input is likely to remain an important factor for determining copyright protection. An AI system shouldn't immediately kill a copyright just by using it. claim, but entirely automatic generation makes a stronger case against interpreting the machine output as a human-written work in the traditional. The study also indicates that deepfakes build a clear connection between intellectual property and cybercrime law.

The legal reaction should encompass identification, privacy, deceit, reputation, and unlawful use of computing resources. Criminal responsibility should rest on already established elements of an offense, not the fact that AI was employed. The report ultimately concludes that India will gain from more explicit regulations governing AI training, synthetic media, provenance and remedies, platform obligations. Such policies should be technology-neutral, proportional, and consistent with constitutional safeguards for speech, privacy, and creativity.³⁵ **CONCLUSION** Artificial intelligence has transformed the practical process of creating and producing digital content. made. The legal system must consequently resolve a series of interconnected questions: who is the author, who owns the output, whether training is infringement, who is liable when synthetic media causes injury, and what? What responsibility do platforms and AI developers have? Indian law already possesses significant instruments in the Copyright Act, 1957, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, data protection laws, and intermediary rules.

They provisions can resolve many of the existing issues, but content produced by AI uncovers areas where more statutory consistency would be improved by clarity. The less favored option is either complete technological independence or over-regulation. Copyright protection must stay linked to genuine human innovation. AI-generated creation should be judged. actual contribution of the human user. Training disputes should be addressed by particular copyright criteria and principles of legal use." Deepfakes and harmful synthetic media should be addressed via privacy, criminal, and intermediary legislation, depending on the specifics of each situation. The Indian framework of the future must provide defined categories, plain obligations, and accessible remedies. Developers and platforms should have adequate accountability systems, and consumers should have an understanding that the AI aid does not relieve liability for illegal action.

Such a strategy can safeguard creators and people without unduly stifling legitimate technological innovation.

22. Limitations of Study

This research is mostly doctrinal and analytical. It deals with the statutory provisions, principles, regulatory advancements and comparative approaches, but does not attempt to assess the frequency of AI-related conflicts using a huge empirical dataset. The technology is also evolving fast,

which means that technical practices and regulatory actions may develop more rapidly than legal doctrine. The document, therefore, focuses on ideas that might be applicable even as specific AI models and platforms evolve. Another problem is the challenge of distinguishing distinct types of AI application. Partial AI-aided editing creation, automated generation, and purposeful impersonation can have extremely different amounts of human legal and control risk. The paper therefore does not regard all AI-generated material as one category. Another rigorous empirical research might look at particular cases and platform practices to determine how courts and regulators are working with these distinctions. The report also recognizes that copyright, privacy, data protection, and cybercrime law protect distinct interests.

One incident may give rise to multiple legal claims, and the decision may turn on facts that cannot be determined by broad principles alone. Future research can thus explore case-specific judicial decisions, enforcement data, and the real working of the complaint and removal systems. These caveats do not detract from the importance of the main point. They point to areas for future doctrinal analysis. Comparative case analysis and research can build upon the present empirical investigations by ongoing assessment of Indian law and regulatory practice.

23. Implementation Strategy of Indian Institutions



Intermediary responsibility and platform safeguards

The legislative framework described in this study will be effective only if it is backed by institutional procedures. Parliament and the relevant regulatory authorities can establish statutory standards, but implementation will also depend upon courts, law enforcement agencies, educational institutions, and technology and professional bodies and corporations. - Each institution has a separate function and should not be given the same responsibilities. Courts can help by creating consistent standards in fact-specific decisions. Copyright in conflicts, courts can consider the extent of the human input, the type of alleged copying, and the input-output connection. In cybercrime issues, courts can distinguish between creation, publication, transmission, and further dissemination. Clear judicial reasoning can slowly lessen uncertainty without needing a new rule for each new AI tool. Law enforcement agencies need technical capacity to investigate synthetic media.

Police officers must be able to preserve digital evidence, discover important platform records, and comprehend the limitations of automated detection system. Training should stress that an AI-detection score alone does not prove who produced or uploaded material. Investigation has to mix technical evidence with the usual evidence about accounts, devices, communications, and motive. Schools also need to adopt practical policies on the usage of artificial intelligence. Students and researchers must be educated about acceptable aid, checking of legal authorities, attribution, and secrecy. The objective should be responsible use rather than a blanket prohibition. Institutions may mandate disclosure of considerable AI aid where appropriate, and can tell the difference between proofreading and substantive generation. Technology corporations should have reasonable safeguards.

These can include provenance systems, reporting channels, user warnings, preservation measures, and mechanisms for recurring abuse. Such protections should include appeals processes since automated systems can misclassify lawful material. Implementation should consequently follow a multi-layer model. Core rights should be set out in statute and obligations. Courts should apply such standards to the facts. Priya Panwar, LL.M., Regulators Research Paper | 17

24. References

The Constitution of India, 1950.² The Copyright Act, 1957.³ Information Technology Act, 2000.⁴ The Information Technology (Intermediary Guideline and Digital Media Ethics Code) Rules, 2021.⁵ The Digital Personal Data Protection Act, 2023.⁶ Bharatiya Nyaya Sanhita, 2023.⁷ The Bharatiya Sakshya Adhiniyam, 2023.⁸ World Intellectual Property Organization, Artificial Intelligence and Intellectual Property Policy Materials (1)⁹. United States Copyright Office, Copyright and Artificial Intelligence Reports and Directions¹⁰. European Union, Regulation establishing harmonized norms on artificial intelligence (EUAI Act).¹¹ United Kingdom legislation and policy documents on copyright and computer-generated works.¹² Relevant Indian judicial rulings on copyright, intermediary responsibility, privacy, Electronic proof and reputation.

25. Authors in AI-Assisted Academic and Legal Writing

The usage of AI tools for drafting, editing, translation, summarization, and research aid is on the increase. In the question of authorship is especially crucial in academic and legal writing since a document that is submitted is the intellectual effort of the individual whose name is on it. Hence, the use of an AI tool must be separated from the transfer of authorship to the tool. A pupil or researcher may use tools to improve grammar or organize thoughts but should continue to exercise substantial intellectual control over the finished output. The trouble starts when the substantial argument, analysis, and conclusions are produced by an AI system with human intervention is quite limited. In such a circumstance the designated person may have trouble in proving that the final statement demonstrates adequate independent intellectual contribution. Institutional academic regulations may also impose disclosure or integrity obligations that are independent of copyright laws.

Accordingly, copyright ownership and academic authorship should not be thought of as being the same concepts.

26. Copyright in AI-Generated Images, Music, and Videos



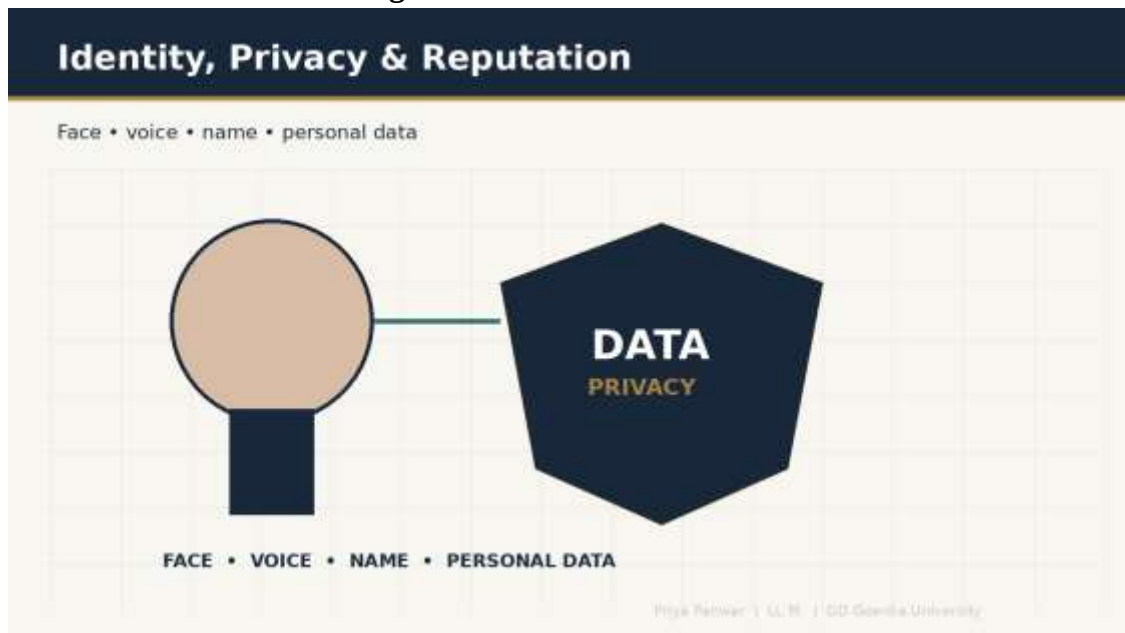
AI-generated works and the copyright question

When conducting legal research, there is a higher risk when artificial intelligence systems construct case names, statute provisions, or quotes correctly. The researcher still has to check the primary legal authorities. AI aid does not substitute for reviewing the original decision, legislation, or official source. The professional framework should so involve significant human evaluation of legal content prior to submission or publication. The right way is to consider AI as an assisting technology, where the human researcher still remains accountable for the choice, the check, the analysis, and the final presentation of the job. This maintains responsibility, allowing for reasonable technology aid. Distinct types of generative content give rise to distinct copyright issues. An image created using AI may have a prompt, reference photos, automated generation, and then human editing.

27. Confidential Information and Trade Secrets in AI

AI Music generation might encompass lyrics, melody, orchestration, and voice synthesizing. Could produce video blend visual scenes, music, speech, and performances. The legal assessment may consequently have to deal with the different components rather than the whole produced as a single, indivisible item. But human editing can play a role. If someone makes a big change to an AI-generated image, chooses certain features, repositions scenes, and creates an original work, the human contribution may be protected even if some underlying stuff is produced by software. The similar idea may be applied to music and video when human creative decisions determine important expressive elements. Another concern is the utilization of the voices or images of existing performers. A synthetic performance could reproduce the identify a genuine person even if the underlying audio recording is not reproduced.

28. AI and Personal Data in Training and the Creation



Identity, privacy and reputation in synthetic media

This leads to a legal difficulty that cannot always be remedied by copyright. Private personality; contractual rights and criminal law based on the conditions of passing off. The proliferation of synthetic media therefore merits a component-based legal examination. Courts should decide What material is protected, who generated it, what was copied, what was altered, and what damage ensued? This method is more accurate than the blanket assumption that all AI-produced content is 100% protected or free from legal obligation. Generative AI also poses threats that aren't fundamentally copyright conflicts. Employees might input private business information, unpublished research, client communications, or proprietary documents to an outside AI service. When information is sent to a third-party system, Problems of storage, processing, retention, and later use arise.⁴⁰

Liability of Developers and Deployers of AI. Trade secret protection often depends on the information being confidential and reasonable actions being taken to preserve secrecy. If an organization is unable to prevent the leaking of secret material, it may undermine its legal and commercial standing;

29. Conclusion



A possible legal and institutional framework for India

Generative artificial intelligence has transformed the practical process through which digital content is created, edited, reproduced, and distributed. The central legal challenge is not simply whether AI was used, but how the law should distinguish meaningful human creativity from largely automated generation and how responsibility should be assigned when synthetic content causes legal harm. Indian law already provides an important foundation through the Copyright Act, 1957, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, data protection principles, and intermediary rules. However, the rapid development of generative AI exposes areas where clearer interpretation and more specific regulatory guidance are required.

For copyright, the most workable approach is to keep human creative contribution at the centre of authorship. Section 2(d)(vi) of the Copyright Act provides a statutory basis for computer-generated works, but its application to modern generative systems requires careful interpretation. A person who develops a detailed creative concept, selects among outputs, substantially edits material, and controls the final expressive form has a stronger claim than a person who merely gives a general instruction and publishes an automatically generated result. The law should therefore avoid both automatic copyright for every AI output and the assumption that every work involving AI is unprotectable.

The problem of AI training must also be considered separately from ownership of outputs. The use of protected works in datasets raises questions concerning copying, licensing, statutory exceptions, contractual restrictions, and the relationship between training material and generated output. These questions should be examined according to the actual acts involved rather than through a single rule that treats all AI training as either lawful or unlawful.

The cyber-crime dimension requires a similar conduct-based approach. AI can be used for legitimate education, research, accessibility, entertainment, and creative work, but it can also make impersonation, fraud, privacy violations, deepfakes, and other harmful conduct easier. Criminal liability should therefore depend on the elements of the particular offence, including the relevant act, knowledge, intention, participation, and available evidence. The mere presence of AI in an activity should not by itself create criminal liability.

The long-term objective should be accountability without unnecessarily restricting innovation. AI should remain a tool that can support human creativity and technological development, while persons and organizations that make or deploy consequential decisions remain responsible for unlawful conduct. A technology-neutral, proportionate, and human-centred legal framework would allow India to protect creators and victims while preserving legitimate uses of artificial intelligence.

30. Limitations of the Study

This research is primarily doctrinal and analytical. It examines statutory provisions, regulatory developments, comparative approaches, and legal principles but does not measure the frequency of AI-related disputes through a large empirical dataset. Because generative AI is developing rapidly, technical practices and regulatory responses may also change faster than established legal doctrine.

The study also recognizes that AI-assisted editing, substantial human-AI collaboration, autonomous generation, and intentional impersonation may involve different levels of legal risk. Future research may examine specific judicial decisions, enforcement data, platform practices, and the practical effectiveness of complaint and removal mechanisms.

31. Implementation Strategy and Future Research

Implementation of the proposed framework would require cooperation between Parliament, courts, regulators, law enforcement agencies, educational institutions, and technology companies. Courts can develop consistent standards for assessing human contribution, copying, publication, and evidence. Law enforcement agencies require technical capacity to preserve digital evidence and investigate synthetic media without treating automated AI-detection scores as conclusive proof of authorship or criminal responsibility.

Technology platforms can strengthen provenance systems, reporting channels, user notices, evidence-preservation mechanisms, and appeal procedures. Educational and professional institutions should promote responsible AI use, verification of legal authorities, confidentiality, attribution, and disclosure where substantial AI assistance is used. Future research should examine AI-generated software code, synthetic performances, personality and voice rights, training-data licensing, cross-border enforcement, and the practical operation of emerging AI regulations.

32. References

1. The Constitution of India, 1950.
2. The Copyright Act, 1957.
3. The Information Technology Act, 2000.
4. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
5. The Digital Personal Data Protection Act, 2023.
6. The Bharatiya Nyaya Sanhita, 2023.
7. The Bharatiya Sakshya Adhinyam, 2023.
8. World Intellectual Property Organization, Artificial Intelligence and Intellectual Property Policy Materials.
9. World Intellectual Property Organization, Generative AI and Intellectual Property Considerations.
10. United States Copyright Office, Copyright and Artificial Intelligence Reports and Guidance.
11. European Union, Artificial Intelligence Act and related policy materials.
12. United Kingdom legislation and policy materials concerning copyright and computer-generated works.
13. Relevant Indian judicial decisions concerning copyright, intermediary liability, privacy, electronic evidence, and reputation.