

Constitutional protection of Personality Rights in the Era of Artificial Intelligence: A Comparative Study of India, EU and the US

Ms. Anmol Arora

Research Scholar, Law, Manav Rachna University

Abstract

The rapid development of artificial intelligence (AI) and synthetic media tools has called into question classical concepts of personality rights, such as the right to one's name, image, voice, etc. In the face of more sophisticated AI-generated content, such as deepfakes and digital clones, this paper analyses how the constitutional and legal protection of personality rights is safeguarded under three jurisdictions—India, the European Union (EU) and the United States. Every jurisdiction is a different model influenced by its constitution, culture, and regulatory evolution.

In India, the evolution of personality rights in constitutional and statutory law are largely fledgling, though courts are beginning to discover them through the doctrine of the right to privacy in Article 21. But the absence of laws or AI regulation meant there were large loopholes that allow the misuse of people's digital identity. By contrast, the EU subscribes to a rights based approach based on dignity and privacy that is enshrined in the EU's Charter of Fundamental Rights, and is implemented through mechanisms such as the General Data Protection Regulation (GDPR) and the proposed AI Act. These systems have some fairly substantial protections against unauthorized use of personal identities, including biometric identifiers and likenesses.

The US is a bit murkier, accommodating personality rights with robust 1st Amendment protections. The right of publicity, a creature of state law, in fact affords commercial control over one's persona, but its utility is significantly lessened by inconsistent enforcement and judges' enforcement due to their veneration of freedom of expression. In the absence of a federal AI law (we have had many AI proposals but no bills passed), and little in the way of state-by-state harmony, AI-generated identity remedies are non-uniform and uncertain.

This comparative analysis uncovers that, although the EU is at the forefront of integrated regulatory responses, India and the USA face constitutional dilemmas and legislative fragmentation. The paper calls for a finely balanced legal ecosystem that respects free expression while guaranteeing dignitary and commercial protections against AI-enabled identity manipulation." It proposes harmonised legislative responses, clarification of the scope of personality rights in the digital sphere, and global cooperation in tackling the challenges that synthetic media technologies present on a transnational level.

Introduction

The era of artificial intelligence (AI) is becoming transformative and it deeply changes societies and laws, in particular with regard to the protection of fundamental rights. Far from a novel problem, AI-generated synthetic media—ranging from deepfakes to avatar creation to voice cloning—raises serious questions

for classical legal doctrines that protect personality. They safeguard one's identity, specifically his or her name, likeness, voice, and/or image, and are based on the recognition of dignity, privacy, and self-determination of values. However these protections are rendered meaningless by the current pace of AI developments meaning that it is increasingly possible to generate lifelike (but fake) images of a person to be used and distributed without their consent, with the potential to amount to defamation, identity theft, intentional infliction of emotional distress, passing off and for commercial gain.

This article engages in a comparative constitutional analysis of the protection of personality rights in India, EU, and in the US, in the age of AI. There is much potential for personality rights protection in India's constitutional law, especially the recognition by the Supreme Court of India of privacy as a fundamental right under Article 21. However, India's law does not have specific AI-related protections and depends largely on the general data protection law that does not adequately cover all risks related to AI.

The EU also offers a strong exemplar—a charter of fundamental rights, and a general data protection regulation (GDPR) that offer the individual tight controls over their own information including most relevantly to synthetic media, their biometric information. The EU is also shaping AI regulation via the proposed Artificial Intelligence Act that seeks to curb high-risk AI applications while respecting fundamental rights. This would be a proactively rights-oriented and "rights-imbued" way of balancing innovation with human dignity.

By contrast, the US rates freedom of speech highest of all under the First Amendment, causing personality rights to be so scattered as to be ineffective. State-level "right of publicity" laws provide some degree of control over commercialized identity, but in the absence of a federal framework and robust speech protections, regulating deepfakes or other AI-created content is challenging. Legally speaking courts are likely to favor speech unless there has been demonstrable commercial harm and this creates lacuna in protection against misuse of AI.

While these specifics differ from one another, on a general level, all three of these jurisdictions suffer from gaps in the law when it comes to dealing with AI and personality rights. This paper proposes creative doctrine and subtle regulation that both honours free expression and elaborates on identity misuse. What is needed to harness the potential of AI, therefore, is a comparative, rights-focused technique to building legal structures to promote human dignity and autonomy in an expanding AI world.

Part I: Conceptual Frameworks and the Disruptive Potential of AI

The rise of artificial intelligence (AI) to produce synthetic media including deepfakes, voice clones, and virtual avatars has redefined how identity and personality are constructed, manipulated, and consumed. These new technologies create complex challenges for established legal systems, especially those that relate to the likes of protection of personality rights--the legal rights that give a person control of and the ability to profit from his or her name, image, voice or likeness, or the specific attributes of his or her identity.

At the heart of this conversation is a fundamental concern: How can the current constitutional and legal order safeguard personality rights when AI technologies can copy, alter, or create personal likeness on a massive, even planetary scale?

• What Are personality rights?

They are more commonly known in some countries as the right of publicity or the personality rights. This set of rights mix concerns of privacy, dignity, and property. Where in some jurisdictions they are "primarily conceived as the extension of the law of privacy and the law of personal autonomy", in others

they are regarded as budget rights encompassing the economic value created through celebrity and recognisability.

In jurisdictions such as the EU, personality rights are foundational rights that come off of the fundamental rights under human dignity and also privacy, which are codified as a constitutional or legal rights in constitutional and super-national entities such as the European Union Charter of Fundamental Rights. By comparison, the United States understands publicity rights primarily as a property interest under the "right of publicity", and the First Amendment often limits the enforcement of publicity rights. India is meanwhile developing its jurisprudence creatively, by adopting interpretation of the concept of 'privacy' under Article 21 of the Constitution, to confer protection of personality rights.

• **Personality Rights Dimensions**

Personality rights are commonly divided into two subsets:

Dignitary or Moral Interests include the protection of dignity, autonomy, and control over one's identity. These interests are rooted in civil law systems, wherein the right to personal characteristics is closely associated with human rights and personal development.

Commercial Interests: This relates to the monetary value attached to an individual's identity – particularly so for public figures, celebrities, and social media influencers. Exploiting personal characteristics for commercial gain, such as through advertising or merchandising, that results in the risk of financial loss or damage to reputation invites legal claims such as those for unjust enrichment or misappropriation.

• **The AI Disruption: Deepfakes, Clones, Digital Doppelgängers**

As AI enabled tools producing hyper-realistic synthetic content have come of age, conventional ideas about identity and personality have been turned upside down. Generative tools, like those that use generative adversarial networks or large language models, can come up with realistic images, videos, audio and text that make it seem as if a real person is in the room, or actually saying something. This occurrence is of special concern:

1. Deepfake pornography has generally been used to target women and public figures without their consent;
2. Bogus endorsements, advertisements with celebrities endorsing goods that they have no relation with;
3. Synthetic influencers, when AI-created personas compromise the boundary between real and artificial individuals;
4. Voice cloning and impersonation that could commonly be used in scams and misinformation campaigns.

In contrast to traditional media manipulation, these variants of artificial identity are scale, available to virtually anyone, and hard to identify or naturally parse. But they can also be employed in more nefarious ways: as tools of harassment, defamation, impersonation or commercial exploitation of individuals — raising immediate legal questions about consent, attribution and culpability.

• **Suffering From the Void of the Law**

By far and away most legislatures are not adapted for dealing with mass and high quality AI manipulation of identity. The tort, IP, and privacy law that do apply to one's image typically target concrete, non-dynamic or temporal abuses of identity. The digital replication of likeness — especially of fictional, satirical or anonymized characters — also taps a legal Gray area. Deepfakes: There are two types of deepfakes - the one that has been generating significant concern at the level of lawmakers and the one that in all likelihood will be difficult to regulate: (1) the Deepfake that affects reputation: deepfakes that do damage to a person's reputation are a false accusation against the person who is portrayed, whether or not

the portrayed is guilty of a crime; (2) the Deepfake that is protected by the First Amendment: say a deepfake of a public figure is being circulated, and it is one of those that, for instance, incorporates the public figure in a satirical skit, then if it causes reputation harm - tough, the speaker wins out because it is free speech.

Another challenge of critical importance is the facility of use combined with the anonymity and the global reach of AIs. Perpetrators are able to produce and circulate image forgeries across countries without an easily traceable source, making the enforcement of the personality rights particularly challenging. Complicating matters further, a number of jurisdictions do not have a specific statutory regime for personality rights or for AI, which would help to provide clarity on these forms of liability, consent, and the use of ethically beneficial AI.

• Legal Roots to AI Identity Abuse

The larger question of what the new legal regime should look like — and how we can strive toward regulating AI's ability to distort identity without infringing other core rights like freedom of speech, innovation and access to technologies — is where academics and policy makers are now deliberating. Some of the legal strategies being discussed include:

- Extending personality rights to the digital avatars and synthetic representations;
- Creating AI-specific laws that will mandate consent and transparency when it comes to generating synthetic identity content;
- Establishing a duty of attribution or disclosure, so that AI-generated material must be labelled as being non-human;
- Creating fair use or transformative use exceptions, particularly for satire, parody or critical speech.

All these proposals involve difficult trade-offs between protecting an individual's identity and preserving speech rights or innovation.

Part II: India – 'Client X' and the Belated Emergence of Personality Rights in the AI Age

The jurisprudence on personality rights in India is still an evolving area of law, especially in today's time, given the rise of AI-generated deepfakes, virtual influencers, and voice clones. India does not have an enacted personality rights statute, unlike many jurisdictions in the world, but rather the courts have stepped to interpret the same based on constitutional principles, principles of tort and intellectual property laws. Though there has been development, especially after recognizing that the right to privacy is a fundamental right, there are still legal voids in dealing with the challenges posed by synthetic identity distortion.

• The Right to Privacy as a Form of Constitutional Recognition

There is no codified right to personality in India. But the edifice of personality rights has been constructed through judicial recognition of rights of privacy and dignity under Art. 21 of the Constitution. The basis for this reasoning lies in the landmark judgment in the case of *Justice K.S. Puttaswamy v. Union of India* (2017)¹, which upheld that the right to privacy constitutes a fundamental right, inclusive of informational privacy, bodily integrity, and decisional autonomy. While the Court did not reference AI or digital identity, the ruling set a crucial precedent for the recognition of notional personality harms in the future.

R. Rajagopal v. State of Tamil Nadu (1994) also in the past recognised an individual's control over the publication of their life story, thereby implicitly acknowledging the right to personal image autonomy. Taken together, these cases appear to establish that a person has a constitutional right to control images of

¹ Justice K S Puttaswamy v Union of India (2017) 10 SCC 1

his or her own identity – an interest that, one would think, could (and perhaps should) be applied to AI-generated images at some point down the line.

- **The tort of privacy and celebrity personality rights**

In the absence of a legislation, an Indian jurisprudence on common law personality rights, especially for celebrities and public figures, have been developed by Indian courts. These rights are traditionally expressed in tort claims such as passing off, defamation, or invasion of privacy, although they are more typically litigated under rubric of misappropriation of goodwill or persona.

*ICC Development (International) Ltd. v. Arvee Enterprises (Delhi 2003)*² is one of the most cited decisions in which the Delhi High Court recognised that the persona of an individual, including that of a sports celebrity is a ‘valuable commercial commodity’. The court stated that “the right of publicity has resulted from the right of privacy and includes any aspect of a person’s identity - his name, personality trait, signature, voice, etc.” This recognition acts as the cornerstone of doctrines that invoke the right of personality in a commercial setting.

The famous case of *Titan Industries Limited v. M/s Ramkumar Jewellers* (2012) was when it was held by the Delhi High Court that unauthorized use of Amitabh Bachchan’s image in an advertisement was fair enough to be restrained, with that being said considering the plaintiff’s right of publicity. In more recent times, in *Anil Kapoor v. Simply Life India* (2023)³, the Delhi high court also handed down a sweeping order of protection to the actor’s voice, image and likeness, as well as those of even the actors of the AI models created from the content, once again signalling the potential to extend personality rights to all manners of digital era content.

- **AI and the Lawless Space**

Despite these jurisprudential strides, however, India’s law remains unprepared to combat AI-specific violations of personality rights. Non-consensual synthetic pornography, political misinformation and fake endorsements are but a few of the end uses of deepfake technology, for example. There is little recourse for victims, who may only have recourse in overlapping provisions under;

*The Information Technology Act, 2000 (IT Act)*⁴ – under Sections 66E, 67 and 67A, dissemination of obscene or private content without consent is criminalized, but these directly neither deal with the advent of synthetic media nor impersonation through means of AI.

Indian Penal Code (IPC) – Sections on defamatory content and online harassment can provide minimal relief.

Copyright Act, 1957 – Provides indirect protection: When AI-generated content infringes artistic or literary works, but not when it is based on only personality traits.

And as of now, the Indian legal framework does not cover full control over digital replicas through any statute, nor does it mandate tech platforms to take down AI generated impersonations of individuals unless they are visibly defamatory or obscene. This lack of regulation is especially hazardous for non-celebrities, whose images can be poached with even less regard for their rights.

- **Insufficient Data and Legislation for AI**

India does not have a specific personal data protection law, but, the *Digital Personal Data Protection Act, 2023*⁵ has been enacted, the requirements of which are yet to be implemented in full. Even if this

² ICC Development (International) Ltd v Arvee Enterprises 2003 (26) PTC 245 (Del).

³ Anil Kapoor v Simply Life India (2023) (Del HC)

⁴ Information Technology Act 2000, ss 66E, 67 and 67A

⁵ Digital Personal Data Protection Act 2023 (India).

legislation is designed to enable individuals to manage their personal data, its target remains data processing and storing - not identity manipulation or synthetic media.

India also doesn't have any broad AI regulations that address transparency, consent or accountability in the creation and spread of deep fakes/cloned voices. Without such legal scaffolding, redress typically requires victims to file civil suits or public interest litigation — procedures that are long, drawn-out and beyond the reach of most.

- **Policy Implications and Next Steps**

The necessity of legislating personality rights in the area of AI is increasingly being acknowledged. Law reform proposals suggest:

- a) Making the right of publicity a law of general applicability, applicable even after death, and protection against digital impersonation;
- b) Proton mail 20M Download AI disclosure mandates, to label synthetic content transparently;
- c) Reinforcing the liability regime for intermediaries, and requiring platforms to remove non-consensual synthetic content;
- d) And by establishing takedown procedures, enabling victims to demand removals of AI-generated likenesses outside the courtroom.

Part III: The European Union — A Rights-Based Regulation Paradigm

Charter of Fundamental Rights and the Right of Personality

EU has constructed a broad constitution of protection of fundamental rights with its core being CFREU. In particular, under Article 7 of the CFREU the rights to respect for private and family life are provided for and under Article 8 data protection. Such provisions emphasize the EU's dedication to the protection of human dignity, autonomy, and privacy, and, thus, provide a strong basis for the protection of personality rights.

In AI, these rights are of particular relevance. AI-generated authored synthetic media (e.g., deepfakes, voice clones, digital avatars) are authored, generated, and shared and may be applied to personal data, including biometric information). The fact that the CFREU specifically mentions data protection as a fundamental right is particularly noteworthy in this context because it offers a constitutional ground for AI technologies which potentially lead to challenges to a person's identity and privacy.

- **GDPR and AI**

Embodiment of the CFREU's principles, the *General Data Protection Regulation (GDPR)*⁶ is a cornerstone of the EU's data protection laws in practice. The GDPR is a rulebook to regulate processing of personal data and contains several provisions relevant for AI systems:

Legality, Fairness and Transparency: Personal data must be processed lawfully, fairly and in a transparent manner, with individuals being informed how their data is used.

- a) **The principle of Purpose Limitation:** Information collected for one purpose may not be used for another purpose without consent (that is, no repurposing of data meant for one context to another).
- b) **Limitation of Data:** collect only that data which is required to achieve a particular goal which minimizes overreach.

⁶ Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1

Mentioned above rights Notices, rectifications and erasure: people have the right to be informed about their data, to have it corrected and to have it deleted – giving them control of their own personal information.

Importantly, the GDPR classifies biometric data—which includes facial images and voice patterns—as special category of personal data, placing it under strict processing requirements. This category is especially pertinent for AI applications using biometric data to create synthetic content. Through inflexible consent rules and processing requirements, the GDPR give people the means to manage their own data, and therefore limits unauthorized use, including some AI-supported personality rights violations.

AI-Specific Regulation on the Horizon:

*AI Act*⁷ As an example of the direction regulation may take, the European Union (EU) has presented a proposal known as the AI Act.

Taking into account the specific risks presented by AI, the EU has proposed the world's first risk-based AI regulation, the Artificial Intelligence Act (AI Act)⁸. The AI Act classifies AI systems into four risk classes – unacceptable, high, limited, and minimal – and related regulatory requirements apply to each of these levels.

High-Risk AI Applications:⁹ The AI Act lists various risk AIs, such as the formation and use of:

- **Biometric Identification and Categorization:** AI applications for remote biometric identification and categorization according to sensitive attributes are included among the high-risk profile solutions, and require special compliance standards.
- **Emotion Recognition:** AI solutions for emotion recognition, especially for use-cases such as workplaces or educational institutions, is considered as a high risk application which might infringe privacy and autonomy.
- **Critical infrastructure and services:** AI systems used for critical infrastructure, education, employment and law enforcement should also be considered high risk as they affects citizens' rights and the proper functioning of society.
- **Prohibited AI Practices** The AI Act¹⁰ prohibits certain AI practices known to carry unacceptable risks including:

Social Scoring: The use of AI for the identification of individuals such as they are associated with a social score, such as a trustworthiness score, or with their personal attribute type that may be used to determine the social behaviour of the individual and the ways the individual can behave that have detrimental treatment and significant negative effects on the individuals.

Manipulative techniques: AI systems that cause distorted behaviour undermining the integrity, or autonomy of a person, including through subliminal techniques, are prohibited.

Unauthorized use of biomarkers nephrectomies: the use of facilitated random data mining throughout the internet or logging cameras biomarkers to create an atlas for facial identification biomarkers is prohibited.

⁷ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM(2021) 206 final

⁸ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM(2021) 206 final.

⁹ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM(2021) 206 final

¹⁰ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM(2021) 206 final

Real-time remote use of biomarkers nephrectomies for identification: the use of real-time remote mass Nerezchur identification, which is used in accessible locations to the public, is prohibited while its use is limited in the defined scenario of law enforcement.

These prohibitions are consistent with the Union mainstream principle and its commitment to its widespread rights and protect the more immediate use of artificial intelligence in areas likely to affect the more impending dignity, tidal privacies, and autonomy.

- **Development of the Court Cases:**

European courts, notably the union court of union, play a central role in the education of the general rights and protections, which include judicial education., including the following cases:

- a. ***Bodil Lindqvist v Åklagarkammaren i Jönköping (2003)***: The CJEU held that referring to individuals on a website and identifying them constitutes processing of personal data, thereby falling within the scope of data protection laws.
- b. ***Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)***: This landmark ruling established the "right to be forgotten," allowing individuals to request the removal of personal data from search engine results under certain conditions.

Part IV: United States – Free Speech Supremacy and Fragmented Coverage

The US stands in stark contrast to the rest of the world when it comes to personality rights, mostly due to its constitutional mandate to protect the freedom of speech, which is guaranteed by the First Amendment. This baseline principle shapes fundamentally how we regulate the confluence of identity, privacy, and personality rights in the United States in the age of the digital, when it is AI-produced synthetic material that increasingly tests the limits of that legal boundary.

- **Constitutional Context and the Publicity Right**

Unlike the European Union, where privacy is considered a fundamental right, the U.S. Constitution doesn't spell out a right to privacy. Instead, the protection of privacy and personality have been established primarily at the state level and over time through common law and statutes, with some constitutional interpretation under the Fourth and Fourteenth Amendments. There is a tension between identity and free speech that is enshrined in the federal constitution's free speech protection.

At the core of many states' doctrines is the right to publicity, protecting an individual's commercial interest in their persona — including names, likenesses, voices, signatures and other unique aspects of one's identity. This right is a property interest redressable in a court of law, as something other than privacy, designed to protect the individual from commercial and not civic invasion of privacy.

There are currently at least 25 states that recognize the right of publicity in some manner. For example, California, Indiana, and Tennessee each grants the right of publicity post-mortem for some period of time following death, but New York possesses more limited privacy-based statutes. For instance, California Civil Code § 3344¹¹ offers protections for unauthorized commercial use of identity, which allows victims to obtain statutory damages and injunctions. Meanwhile, New York Civil Rights Law §§ 50–51¹² target intrusions of privacy and false endorsements, but afford more limited protection.

- **Growing Pain of AI Created Synthetic Content**

The explosive development of the AI, such as the deepfake technology, voice cloning, or the synthetic

¹¹ California Civil Code § 3344 (West 2023)

¹² New York Civil Rights Law §§ 50–51 (McKinney 2023)

avatars further readjust the entire conventional personality rights framework. AI offers the possibility to make extremely realistic, artificial depictions of human beings, often without need of an explicit commercial broker or the consent of the person depicted.

Historically, the traditional right of publicity does not fit well with synthetic media, which, when it flows freely on the internet, can obscure the distinction between expression, parody, misinformation, and exploitation. For example, when an AI-produced video shows a celebrity promoting a product without their consent, it raises the complicated question of how applicable the laws available to intervene in such a case are. These hypotheticals call into question the core element of human agency and objective relevance present in many publicity claims.

• A Patchwork of Laws and Regulations

Whereas the EU obviously has the GDPR and the forthcoming AI Act¹³ to protect user data, the U.S. lacks a federal framework of its own to regulate data privacy when it comes to AI-generated synthetic media. The legal regime is not unified, comprehensive, and proactive; rather, it is piecemeal, piecemeal, and reactive.

Relevant federal statutes that are only tangential related to AI and identity:

*Lanham Act*¹⁴ (15 U.S.C. §§ 1051 *et seq.*), which focuses mainly on trademarks, provides for false endorsement claims in which a likeness is utilized to suggest that a person is a commercial endorser, but does not generally protect personality rights.

*Video Privacy Protection Act (VPPA)*¹⁵ tries to protect consumers' privacy in the context of video rental records, but is unlikely to have minimal impact on the misuse of AI synthetic identities.

Unauthorized access to computers is a crime under the *Computer Fraud and Abuse Act*,¹⁶ but it is of limited applicability to synthetic media.

The FTC focuses on fraudulent and unfair trade practices. While the FTC has initiated AI-related consumer harm investigations, no clear guidance or rules related to synthetic identity manipulation have been issued.

And at the state level, some areas are taking a more proactive approach:

California and Texas have outlawed non-consensual deepfake pornography and spreading synthetic videos designed to influence elections.

Virginia State The statute gives room to civil remedies for victims of deepfake pornography.

NY recently modernized its approach to same via the passage of its 2020 'digital replica' and post-mortem right of publicity statute, giving rights of personality similar to what we have observed elsewhere from CA past years.

The state measures are steps in the right direction, but they are hit or miss, and they do little to protect non-wealthy individuals, rather than celebrities and public figures.

Law Dispatches on Stigmatisation 60· P Rozendaal, The Principle of Equality and Internet Hate, Hate Speech another Forms of Stigmatisation, 1–12· AGW Hartmann, Can the Law Cure the Violence of Law speak?

¹³ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM(2021) 206 final

¹⁴ 15 USC §§ 1051–1141n (Lanham Act)

¹⁵ 18 USC § 2710 (Video Privacy Protection Act).

¹⁶ 18 USC § 1030 (Computer Fraud and Abuse Act).

The U.S. grapples with a core constitutional tension: how to shield people from AI-enabled manipulation of their identities, without trampling the Great Amendment's strong protections for freedom of speech. Proponents of stronger personality rights underline the dignitary, emotional and reputational injuries that arise from synthetic media, such as harassment, reputational damage, loss of personal control. They demand that legislation do the same at a federal level, which recognized not only personality rights, but AI development and deliver meaningful remedies to victims.

In the other camp, defenders of free speech caution that overly broad regulations will chill artistic expression, satire, journalism and political speech — all central to democratic engagement. At a time when creating in digital media is open to all, these advocates emphasize the need for viewpoint neutrality and the dangers of legislation that could chill innovation or lawful transformative uses..

Part V: Comparative and Reflective and Future Prospects

• Similarities and Differences

In India, the EU, and the US, the constitutional guarantee of personality rights face the most severe test in the era of artificial intelligence. Although these countries share in common the values of human dignity, autonomy and self-determination, their constitutional cultures and legal designs result in significantly contrasting positions.

In the EU, the right-based and preventive regime prevailed, based on human dignity and privacy. The CFREU and the GDPR provide strong protections for personal data and identity, which new creations like the Artificial Intelligence Act take further into the AI space. The EU model operates on the basis of preventive governance, placing the onus on AI developers and deployers to ensure their systems are in line with human rights norms.

In the other extreme, First Amendment culture tends to dominate constitutional culture in the U.S., where expressive freedoms generally triumph over personality-based claims. There is a right of publicity, but it is a patchwork, with protection not uniform between states, and restricted by judicial deference to free speech. With no national standard for data and AI regulation in place in the U.S., tackling the complex threat of synthetic media is a tough nut to crack in any sort of consistent or comprehensive way.

India, meanwhile, falls somewhere in between. Its maturing case law including its post Puttaswamy, has initiated the constitutionalisation of privacy and dignity as fundamental rights. However, India does not have any particular laws or regulations focusing on AI or personality rights. The constitutional affirmation of personality rights are still rudimentary, while avenues for enforcement are inadequate or closed to many. This vacuum of oversight is a ripe environment for AI-based identity misuse which has little to no legal remedy.

• Toward Doctrinal Creation and Reform

Emergence of AI-synthesized media such as deepfakes pose unique threats to personal identity, reputation, and mental health. Meeting these challenges will require not just doctrinal innovation, but regulatory reform, too.

The first is that personality rights should be expressly acknowledged as basic constitutional rights, rooted in human dignity and autonomy. The agreement would set a clear normative line, against which legislation and policy could be developed.

Second, legal norms of consent, authenticity, and harm must be bespoke for synthetic media. The prevailing doctrines do not apply to situations involving uncertain consent, partly real and partly fabricated content, or reputational rather than monetary injury.

Third, we need to reform our data protection and IP laws to take account of AI-specific protections, especially in relation to biometric and identity data. This involves transparency in the production of AI-generated content, labelling between real and synthetic media and effective mechanisms of resolution. Enforcement In the AI context, enforcement tools should be accountable, explainable, and place responsibility on platforms. Regulation should aim for the right balance of individual rights and freedom of expression with flexible, culture-specific criteria that prevent excessive limitation.

- **The role of multilateral cooperation and global norms**

AI technologies are not limited by national boundaries. The harm of content produced in one jurisdiction is felt in another, such that state-centric systems of regulation are exposed. Accordingly, the protection of the personality rights in the AI age calls for int'l cooperation of harmonizing the standards and developing the global norms.

As appealing a template as the EU's full-bore, rights-based regulation is, it alone can't fix the jurisdictional symptoms of borderless AI tech. We need a world-wide conversation about how to harmonize competing constitutional values – free speech and privacy – across different legal traditions. In international human rights agreements like the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, personality rights should be amended or reasonably explained to include personality rights in relation to the application of AI. This would encourage a common normative basis that is rooted in human dignity and autonomy and that could establish the groundwork for globally pertinent ethics guidelines for AI.

Taken together, securing personality rights in an AI age will depend not only on domestic legal developments, but also on transnational cooperation, persistent normative dedication, and regulatory agility to respond to the novel issues posed by a digital environment in rapid flux.

Conclusion

Artificial intelligence is a turning point for the constitutionally protected rights of personality. India, the European Union, and the United States highlight the differential constitutional responses reflecting varied legal cultures and normative preferences. Privacy, dignity and free expression rights provide important foundations, they're just not enough in the face of the AI-driven scale, speed and sophistication of identity manipulation. This Article has contended that clear doctrinal principles, legislative change, and dynamic regulation are necessary to build strong personality rights for the AI era. A balance-regarding perspective is critical — weighing respect for individual autonomy against collective interests in free expression and innovation. Constitutional law should not be stuck in the past when it comes to technology. Instead, it must adapt, so that the right to autonomous control over one's identity and image, lest it become merely a form of human dignity, remains steadfastly protected. In this way, the manners in which legal systems can protect the personal integrity of those who live their lives in a constantly more artificial digital world are analysed.