Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

Article 21 in the Generative Era: Protecting Personal Identity and Privacy against AI Infringements in India

Dr. Shashi Nath Mandal, WBES

Associate Professor of Law
Government Centre of Legal Education
Govt. of West Bengal, Chinsurah, Hooghly, West Bengal

Abstract:
The rapid deployment of Generative Artificial Intelligence (AI) and hyper-realistic synthetic media architectures has triggered deep disruptions within India's constitutional landscape. Under Article 21 of the Constitution of India, the Right to Privacy stands as a sacrosanct fundamental right, protecting individual dignity and personal autonomy. However, technologies like deepfakes, voice cloning, and autonomous algorithmic profiling present severe threats by separating digital representation from true user consent. This research paper significantly expands upon current legal literature by examining the critical vulnerabilities within India's newly enacted and amended statutory matrix—including the Digital Personal Data Protection (DPDP) Act, 2023, the Information Technology Act, 2000, the Consumer Protection Act, 2019, and the Bharatiya Nyaya Sanhita (BNS), 2023. Moving beyond localized issues, this paper introduces a thorough four-way comparative analysis with the regulatory regimes of the United Kingdom, the United States, and Canada. By evaluating risk-based, copyright-led, and consumer-welfare models alongside emerging Indian judicial precedents protecting celebrity 'personality rights,' this article outlines necessary statutory and institutional reforms required to safeguard human identity against automated infringement.

Keywords: Artificial Intelligence, Deepfakes, DPDP, Cognitive liberty, Privacy, Identity Theft, Personal Liberty.

1. Introduction

The digital frontier of the twenty-first century is being fundamentally redrawn by the swift evolution and mass proliferation of Generative Artificial Intelligence. Systems once limited to academic environments—such as high-fidelity generative adversarial architectures, cross-modal neural voice synthesizers, and self-improving algorithmic profiling networks—have democratized creation across the globe. However, this technical leap has brought with it an asymmetric threat matrix. At the center of this shift lies the 'deepfake', a visual or auditory creation born from Generative Adversarial Networks (GANs). In these systems, two

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

neural structures—the generator and the discriminator—engage in a continuous algorithmic game to build synthetic media that is virtually indistinguishable from authentic captures. While positive applications exist within interactive digital entertainment and simulated pedagogy, the rapid weaponization of synthetic media has vastly outpaced structural defenses, causing profound legal anxieties globally and uniquely within India.[1]

In modern constitutional jurisprudence, privacy can no longer be limited to the classic formulation of 'the right to be let alone.' Instead, it must be understood as a multi-layered right that safeguards informational self-determination, the continuity of personal identity, cognitive liberty, and digital bodily autonomy. Generative AI disrupts this understanding. By recreating and altering an individual's visage, voice, emotional patterns, and unique behavioral markers without consent, generative models separate a person's biological reality from their public digital representation. This causes an unprecedented 'contextual collapse.' In this environment, an individual's identity can be completely disconnected from their personal agency, exposing them to unique forms of technological exploitation, synthetic defamation, and systematic dignity erasure.[2]

2. The Constitutional Matrix of Privacy in India

The bedrock of privacy protections in the Republic of India is rooted in Article 21 of the Constitution, which mandates that 'no person shall be deprived of his life or personal liberty except according to procedure established by law.' For decades, the Supreme Court of India adopted an expansive interpretative approach, reading various implied guarantees into this short phrase, including the right to livelihood, clean environments, and personal reputation. This evolution culminated in the historic nine-judge bench decision in ***Justice K.S. Puttaswamy v. Union of India***[3]. The Court unanimously recognized privacy as a fundamental constitutional right, declaring it an essential component of life, liberty, and human dignity under Part III of the Constitution.[4]

The Puttaswamy paradigm establishes that any state or private intrusion into an individual's private sphere must strictly clear a rigid four-pronged hurdle: legality (the presence of clear statutory law), necessity (pursuit of a legitimate state aim), proportionality (a rational, minimal nexus between the objective and the chosen mechanism), and structural procedural safeguards against administrative overreach. Within the universe of Generative AI, this multi-layered standard serves as the ultimate metric for checking both legislative gaps and technical overreach. When algorithmic models distort, manipulate, or steal an individual's personal identity, the legal harm crosses from a mere tortious or commercial wrong into a direct violation of their fundamental right to informational self-determination and identity sovereignty.[5]

---

1 Danielle Keats Citron & Robert Chesney, 'Deepfakes and the New Disinformation Disruptions', California Law Review, Vol. 108, 2020, p. 1753

2 Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy', Harvard Law Review, Vol. 4, No. 5, 1890, p. 193.

3 (2017) 10 SCC 1: AIR 2017 SC 4161

4 K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

5 Id. at Paragraph 325, per Chelameswar, J.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

Furthermore, AI-driven identity manipulation presents a direct threat to the right to reputation and individual dignity, both of which are core elements of Article 21. In ***Subramanian Swamy v. Union of India***[6] (2016), the apex court affirmed that an individual's reputation is an intrinsic element of the constitutional right to life. When deepfake algorithms place a person's likeness into illegal, compromising, or highly embarrassing settings, severe and permanent harm occurs instantly across global networks. This harm is amplified because digital systems lack contextual memory, making the loss of dignity permanent.[7]

3. The Technological Threat Matrix & Gendered Dimensions

To accurately diagnose the legislative vulnerabilities in current laws, one must examine the specific computing architecture that powers generative technologies. Legacy manipulation tools relied on manual editing, which left clear digital artifacts that forensic teams could easily detect. Modern Generative AI, however, relies on deep learning structures, specifically GANs and diffusion-based models. A GAN functions through a continuous internal feedback system: a generator network constructs increasingly accurate fake media, while a discriminator network checks those generations against genuine datasets to uncover errors. This competitive loop runs millions of times until the discriminator can no longer differentiate between the biological original and the synthetic clone. [8]

The most harmful manifestation of this technology is the proliferation of non-consensual deepfake pornography (NCDP). Global empirical data shows that over ninety percent of online deepfakes are pornographic, and they target women almost exclusively. This reality highlights the gendered nature of digital weaponization. By mapping a woman's face onto sexually explicit media without consent, these tools inflict severe psychological harm, enforce social isolation, and destroy professional lives. This represents an unmitigated attack on bodily privacy and digital safety. Traditional concepts of bodily integrity must expand to encompass digital avatars and representations. The psychological and societal harm caused by digital violations closely mirrors the trauma of physical violence, showing that digital identity theft has real-world consequences.[9]

4. Comprehensive Evaluation of India's Legislative Framework

4.1. The Digital Personal Data Protection (DPDP) Act, 2023

As these complex threats scale across India's massive internet user base, the statutory architecture is facing unprecedented stress. India's core data protection statute is the Digital Personal Data Protection (DPDP) Act, 2023. While the Act sets up a formal framework by establishing 'Data Principals' (individuals) and 'Data Fiduciaries' (processing entities), it contains an existential loophole regarding Generative AI.

---

6 (2016) 7 SCC 221 : AIR 2016 SC 2728

7 Subramanian Swamy v. Union of India, (2016) 7 SCC 221.

8 Ian Goodfellow et al., 'Generative Adversarial Networks', Communications of the ACM, Vol. 63, No. 11, 2020, p. 139.

9 Report of the UN Special Rapporteur on violence against women, 'Online violence against women and girls from a human rights perspective', A/HRC/38/47, 2018.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

Section 3(c)(ii) states that the Act's provisions do not apply to personal data that is 'made available by the Data Principal' or is 'publicly available under any law.' This exemption leaves individuals vulnerable. Large Language Models (LLMs) and diffusion engines regularly scrape public profiles, social media feeds, and internet registries to train their systems. Because this data is considered ‘publicly available’, AI developers can freely harvest facial profiles, voice clips, and behavioral data without consent, bypassing the DPDP Act's notice and consent mandates.[10]

4.2. The Information Technology Act, 2000 & Intermediary Liability

Similarly, the Information Technology (IT) Act, 2000, is proving inadequate against modern generative tools. Section 66E criminalizes the unauthorized capturing or sharing of images of an individual’s private areas, but its wording struggles when applied to completely synthetic media where no physical space was actually compromised. Sections 67 and 67A penalize the transmission of obscene or sexually explicit content, but they focus on classic obscenity standards rather than the core violation of personal privacy and identity theft. The IT Rules 2021 (amended in 2023) try to address this by ordering social media intermediaries to take reasonable steps to block misinformation and digital impersonations. However, the ‘safe harbor’ regime under Section 79 of the IT Act still shields major platforms. Intermediaries are generally immune from liability until they receive ‘actual knowledge’ through a formal takedown notice. In the hyper-viral world of deepfakes, the hours or days required to process these notices allow synthetic media to spread widely, making post-facto removals largely ineffective.[11]

4.3. The Bharatiya Nyaya Sanhita (BNS), 2023

On the criminal justice front, the Bharatiya Nyaya Sanhita (BNS), 2023—which replaced the Indian Penal Code—introduces updated provisions but lacks technical specialization. Statutes targeting forgery (Section 336), criminal defamation (Section 356), and actions insulting the modesty of a woman (Section 79) are frequently used to prosecute deepfake creators. However, these provisions rely on traditional, physical standards of evidence, intent, and documentation. They struggle to address the automated, decentralized nature of Generative AI, where creators can remain anonymous, route their activities through multiple jurisdictions, or use automated scripts to generate and spread content.[12]

4.4. Expanding the Legal Web: Consumer Protection & Copyright Lacunae

The legal vulnerabilities extend into commercial and economic laws. The Consumer Protection Act, 2019, penalizes misleading advertisements and unfair trade practices under the Central Consumer Protection Authority (CCPA). When AI-generated deepfakes and voice clones are used to fake celebrity endorsements or commit financial fraud, they harm consumer trust. However, the Act lacks clear procedures to hold the developers of autonomous generative tools liable, focusing instead on traditional advertisers and endorsers. Furthermore, the Copyright Act, 1957, contains major gaps regarding AI training data. Under current Indian copyright law, fair dealing exemptions (Section 52) are vague regarding whether scraping copyrighted artistic works, portraits, and performances to train commercial AI

[10] Digital Personal Data Protection Act, 2023, s. 3(c)(ii).

[11] Information Technology Act, 2000, ss. 66E, 67, 67A; IT Intermediary Rules, 2021, Rule 3(1)(b).

[12] The Bharatiya Nyaya Sanhita, 2023, ss. 79, 336, 356.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

models constitutes infringement. This lack of clarity deprives creators of economic and moral rights over their digital expressions.[13]

5. Global Standards & Cross-Jurisdictional Comparative Analysis

To build an effective regulatory response, Indian policymakers must analyze international legislative strategies. Different jurisdictions have developed distinct regulatory philosophies, ranging from proactive risk-management systems to copyright-centric frameworks and consumer welfare models.

Regulatory Dimension	European Union (EU)	United Kingdom (UK)	United States (US)	Canada
Primary Legislative Strategy	Proactive, risk-based classification via the comprehensive EU AI Act (2024).[14]	Decentralized, sector-specific model led by the Online Safety Act 2023 and existing regulators.[15]	Decentralized, state-level criminal statutes balanced against strong First Amendment rights.[16]	Proposed Artificial Intelligence and Data Act (AIDA) under Bill C-27.[17]
Synthetic Media & Deepfakes	Mandatory machine-readable watermarking and transparency logs under Article 52.[18]	Criminalizes creation/sharing of non-consensual deepfakes under the Online Safety Act.[19]	State-level laws (e.g., CA, NY) criminalizing political and pornographic deepfakes.[20]	AIDA mandates risk-mitigation strategies for general-purpose systems.[21]
Data Scraping Policies	Strict opt-out mechanisms for text/data mining	Favors pro-innovation data mining, but regulated by UK	Broadly protected under the 'Fair Use' doctrine,	Regulated by PIPEDA; requires clear consent for processing

[13] The Consumer Protection Act, 2019, s. 2(47) and The Copyright Act, 1957, s. 52.

[14] European Union Artificial Intelligence Act (formally designated as Regulation (EU) 2024/1689)

[15] Online Safety Act 2023

[16] Counterman v. Colorado, 600 U.S. 66 (2023) : 216 L. Ed. 2d 775 (2023)

[17] Artificial Intelligence and Data Act, which is proposed as Part 3 of Bill C-27 (named the Digital Charter Implementation Act, 2022)

[18] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, commonly known as the EU Artificial Intelligence Act (EU AI Act).

[19] The Online Safety Act 2023 of the United Kingdom (via amendments integrated into the Sexual Offences Act 2003)

[20] California Statues: New York Statutes in USA.

[21] Artificial Intelligence and Data Act (AIDA)

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

	under Copyright Directives.	GDPR's purpose-limitation rules.	creating major privacy gaps.	publicly scraped info.
Enforcement Mechanism	EU AI Office backed by substantial global turnover fines (up to 7%).	Ofcom acts as the primary enforcement body for online intermediary platforms.	Federal Trade Commission (FTC) handles algorithmic deception and fraud.	Proposed AI and Data Commissioner with direct enforcement and penal powers.

5.1. The European Union Model: Proactive Transparency

The European Union's Artificial Intelligence Act (EU AI Act), passed in 2024, stands as the world's most comprehensive risk-mitigation legal system. Rejecting reactive litigation, the EU framework uses a clear, risk-based classification model that bans unacceptably dangerous AI systems while subjecting 'high-risk' frameworks to strict oversight. Crucially, Article 52 of the Act places direct transparency requirements on generative system developers. Providers must ensure that all synthetic audio, visual, text, or video outputs are permanently marked in a machine-readable format as artificially generated. This enforcement of mandatory watermarking and comprehensive logs ensures that citizens can clearly identify synthetic media, protecting the digital public square from identity deception.[22]

5.2. The United Kingdom Model: Intermediary Accountability

The United Kingdom has chosen a pro-innovation, sector-led regulatory path. Rather than creating a single centralized AI agency, the UK empowers existing regulatory bodies—such as the Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA)—to enforce common principles within their fields. However, the passing of the Online Safety Act 2023 marked a major shift towards active platform safety. This statute explicitly criminalizes the creation and distribution of non-consensual deepfakes. It places a statutory 'duty of care' on digital intermediaries, forcing tech platforms to proactively find, block, and remove intimate synthetic media, shifting the regulatory focus from individual creators to platform compliance.[23]

5.3. The United States Model: Sectoral Fragmentation & Constitutional Conflict

The United States continues to rely on a highly fragmented, sector-specific regulatory approach. At the federal level, the Federal Trade Commission (FTC) uses its consumer protection powers to penalize deceptive AI practices, including unauthorized voice cloning used in financial scams. Concurrently, individual states have passed independent laws; California and New York, for example, have criminalized non-consensual deepfake pornography and banned synthetic media speech protections of the First Amendment, making comprehensive federal legislation difficult to pass.[24]

[22] European Parliament, Regulation (EU) 2024/1689 (Artificial Intelligence Act), 2024, Articles 5, 52(3).

[23] United Kingdom Parliament, Online Safety Act 2023, c. 38, Section 41.

[24] Harvard Law Review, 'Regulating GenAI and the Right of Publicity in the Digital Ecosystem', Vol. 137, No. 4, 2024, p. 1210.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

5.4. The Canadian Model: Comprehensive Accountability

Canada's regulatory blueprint is centered around Bill C-27, which includes the proposed Artificial Intelligence and Data Act (AIDA). AIDA introduces a robust regulatory system focused on 'high-impact' AI models. It requires developers to establish comprehensive risk-mitigation strategies, run continuous equity audits, and maintain clear transparency data. For synthetic media, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) maintains that scraping personal data from public spaces without clear, purpose-limited consent violates data protection principles, establishing a strict barrier against unchecked algorithmic harvesting.[25]

6. Judicial Trends and Enforcement Roadblocks in India

As legislative bodies update statutory laws, the Indian judiciary has increasingly stepped in to protect individual autonomy using common-law principles. This is visible in the rapid rise of celebrity 'personality rights' litigation in various High Courts. In landmark interim rulings such as ***Anil Kapoor v. Simply Life India & Ors.***[26] and ***Amitabh Bachchan v. Rajat Nagi and Ors.***[27], the Delhi High Court restrained digital platforms, tech developers, and anonymous entities from using AI to clone these celebrities, voices, faces, or signature styles without a license. The Court recognized that an individual's identity holds intrinsic moral and economic value that cannot be exploited under the guise of technical freedom.[28]

Despite these positive judicial steps, ordinary citizens face immense hurdles when trying to enforce their rights. The decentralized nature of internet communication, the ease of maintaining anonymity online, jurisdictional boundaries, and the lack of digital forensics capabilities within local cyber cells create significant barriers. While high-profile individuals can secure rapid injunctions from High Courts, ordinary victims of deepfake manipulation face prolonged delays in cyber-cell processing, allowing harmful synthetic media to remain online indefinitely.[29]

7. Judicial Interventions

7.1. Constitutional & Bodily Autonomy

- ***K.S. Puttaswamy (Aadhaar-5J) v. Union of India***[30]***:*** Reaffirmed informational self-determination and informational privacy, establishing that personal identity data cannot be processed without strict consent and statutory procedural safeguards.

---

25 Parliament of Canada, Bill C-27: The Digital Charter Implementation Act, 2022 (Part 3: Artificial Intelligence and Data Act).

26 CS (COMM) 652/2023, decided by the Delhi High Court on September 20, 2023

27 CS(COMM) 819/2022

28 Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi HC); Amitabh Bachchan v. UOI, CS(COMM) 819/2022.

29 Justice B.N. Srikrishna Committee Report, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians', Ministry of Electronics and Information Technology, 2018

30 (2019) 1 SCC 1

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

- ***Navtej Singh Johar v. Union of India[31]:*** Expanded the scope of Article 21 by declaring that individual autonomy, personal identity, and dignity are inviolable constitutional guarantees that shield an individual against societal and technological subjugation.
- ***Selvi v. State of Karnataka[32]:*** Established the doctrine of **cognitive liberty** and mental privacy under Article 20(3) and Article 21, creating an essential precedent against the non-consensual algorithmic extraction and simulation of psychological and behavioral markers.
- ***Justice K.S. Puttaswamy (Retd.) v. Union of India[33]*: (Concurring Opinion of Chandrachud, J.):** Explicitly noted the "right to be forgotten" and informational control as elements of privacy, directly applicable to synthetic data training sets.

7.2. Statutory Intermediary Liability & Digital Safety (To expand Section 4.2)

- ***Shreya Singhal v. Union of India[34]:*** Read down Section 79(3)(b) of the Information Technology Act, 2000, establishing that an intermediary must receive a court order or government directive ("actual knowledge") before safe-harbor immunity is revoked. This ruling creates the critical enforcement bottleneck where viral deepfakes spread unchecked before victims can obtain formal court orders.
- ***Praful Patel v. Western Airlines[35]:*** An early foundational tort authority establishing that unauthorized appropriation of an individual's likeness constitutes an actionable invasion of privacy and tortious infringement.

7.3. Personality Rights, AI Voice Cloning & Digital Likeness

- ***Arijit Singh v. Codible Ventures LLP & Ors.[36]:*** Landmark interim ruling directly confronting generative AI voice cloning. Justice Chagla held that unauthorized AI voice-conversion models, synthetic timbre replication, and digital voice-swapping infringe upon an artist's personality rights and jeopardize their livelihood under common-law tort and Article 21 principles.
- ***Jaikishan Kakubhai Saraf alias Jackie Shroff v. The Peppy Store & Ors.[37]:*** Restrained commercial platforms and AI bot operators from exploiting an actor's name, voice, images, and signature mannerisms/catchphrases without authorization, while also balancing commercial exploitation against parody and artistic expression.
- ***D.M. Entertainment Pvt. Ltd. v. Baby Gift House[38]:*** Foundational Indian authority that introduced the tort of passing off and dilution through unauthorized commercial appropriation of a celebrity's persona and likeness (Daler Mehndi dolls).

[31] (2018) 1 SCC 1

[32] (2010) 7 SCC 263

[33] (2017) 10 SCC 1

[34] (2015) 5 SCC 1

[35] 1976 SCC OnLine Guj 43

[36] Interim Application (L) No. 23560 of 2024 in Com IPR Suit (L) No. 23443 of 2024 (Bombay HC)

[37] CS(COMM) 389/2024 (Delhi HC)

[38] 2010 SCC OnLine Del 4790

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

- ***ICC Development (International) Ltd. v. Arvee Enterprises[39]:*** Recognized that persona and right of publicity inhere only in an individual human being as part of their personal autonomy, rather than non-living or corporate entities.
- ***Deepa Jayakumar v. A.L. Vijay[40]:*** Examined post-mortem privacy and personality rights, affirming that personality rights are rooted in Article 21 dignity and generally extinguish upon death unless distinct commercial/copyright exploitation survives.

8. Conclusion

The rise of Generative AI represents an existential turning point for Indian constitutional law. As automated models grow capable of flawlessly cloning human identity, the protections of Article 21 must evolve from a historic shield against physical state overreach into an active regulatory tool governing the digital world. To preserve individual dignity, India must transition from a reactive legal stance to a proactive, technologically grounded framework. To achieve this, following recommendations are made:

- ***Cryptographic Watermarking Mandates:*** Legislate a strict requirement forcing all consumer-facing Generative AI engines operating in India to embed permanent, cryptographic watermarks and metadata tags into their outputs to ensure clear traceability.
- ***Reforming the DPDP Act Exemption:*** Amend Section 3(c)(ii) of the DPDP Act, 2023, to narrow the 'publicly available data' exemption, ensuring that harvesting personal data for commercial AI training requires explicit, purpose-limited consent.
- ***Accelerated Takedown Windows for Intermediaries***: Amend the IT Rules to create a strict, mandatory 12-hour takedown window for non-consensual intimate synthetic media, shifting the legal focus toward automated platform scanning.
- ***Establishing Digital Forensic Tribunals:*** Create fast-track judicial cells staffed by legal and technical experts to resolve identity theft cases quickly, bypassing delayed traditional cyber-cell infrastructure.

REFERENCES:

A. Primary Sources: Statutes & Treaties

1. The Constitution of India, 1950.
2. The Digital Personal Data Protection Act, 2023 (India).
3. The Information Technology Act, 2000 (India).
4. The Bharatiya Nyaya Sanhita, 2023 (India).
5. The Consumer Protection Act, 2019 (India).
6. The Copyright Act, 1957 (India).
7. Regulation (EU) 2024/1689 (European Union Artificial Intelligence Act).
8. Online Safety Act 2023 (United Kingdom).

[39] 2003 (26) PTC 245 (Del)

[40] (2021) SCC OnLine Mad 2642

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 5, September-October 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i05.1539

9. Bill C-27: Artificial Intelligence and Data Act (Canada).

B. Primary Sources: Judicial Precedents

1. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
2. Subramanian Swamy v. Union of India, (2016) 7 SCC 221.
3. Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi HC).
4. Amitabh Bachchan v. Telecom Regulatory Authority of India, CS(COMM) 819/2022 (Delhi HC).

C. Secondary Sources: Books & Government Reports

1. M.P. Jain, Indian Constitutional Law (8th ed., LexisNexis 2018).
2. Justice B.N. Srikrishna Committee Report, 'A Free and Fair Digital Economy', MeitY, 2018.
3. Law Commission of India, Report No. 267 on Hate Speech and Synthetic Misinformation.

D. Secondary Sources: Academic Journals

1. Danielle Keats Citron & Robert Chesney, 'Deepfakes and the New Disinformation Disruptions', California Law Review, Vol. 108, 2020.
2. Harvard Law Review, 'Regulating GenAI and the Right of Publicity in the Digital Ecosystem', Vol. 137, No. 4, 2024.
3. Ian Goodfellow et al., 'Generative Adversarial Networks', Communications of the ACM, Vol. 63, 2020.