Page 3242 - 3252 **DOI:** *https://doij.org/10.10000/IJLMH.1110214*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

The Jurisprudence of Digital Identity: Reconciling Privacy with the Threat of Identity Theft through Deepfake

MEHAKPREET KAUR[1]

ABSTRACT

It is often said that 'a picture conveys a thousand words.' But Deepfakes raise questions of personal reputation and control over one's image on the one hand and freedom of expression on the other. This will have a significant impact on user's privacy and security. The Deepfake technology poses novel ethical dilemmas and challenges that demand urgent solutions. Violations of privacy are a foremost concern. Using someone's likeness without consent to create fake intimate imagery or videos infringes on their right to privacy under Article 21 of the Indian Constitution. Deepfakes often non-consensually expose people's private lives by depicting them in compromising situations, thus infringing Article 21 of a person. Identity theft enabled by hyper-realistic deepfakes can allow fraudsters to impersonate unsuspecting individuals. Voice cloning to mimic financial executives has already been used for cybercrime. Such breaches of privacy must be addressed to protect citizens. The viral spread of deepfakes on social media can ruin reputations and lives within minutes. Even if proven false later, the stigma and trauma remain. This article discusses the role played by Judiciary in defining the scope of identity theft and outlining measures to protect victims' rights through landmark judgments and legal precedents. It also emphasis the concerted efforts by stakeholders, including government agencies, law enforcement authorities, and service providers, essential to combat this growing menace effectively and safeguard individuals' right to identity.

I. INTRODUCTION

Identity theft via DeepFake poses a constant threat as it violates the Right to Privacy of individuals. Described as the latest form of theft, it involves stealing a person's identity, thereby encroaching upon their Right to Personality. The risk of harming integrity of personal identity and misuse of it as well as the risk of privacy invasion and function creep represent major issues.[2] In the case of integrity of the subject's identity, during the identity theft or loss more

[1] Author is a Research Scholar at Department of Laws, Guru Nanak Dev University, Amritsar, India.

[2]CHRISTIAN RATHGEB, RUBEN TOLOSANA, *etal.,* HANDBOOK OF DIGITAL FACE MANIPULATION AND DETECTION—FROM DEEPAKES TO MORPHING ATTACKS 471 (2022).

 [ISSN 2581-5369]

than privacy will be harmed, the subject could be refused access to services, lose control over their identity, and face damages which are done in their name. Victims of identity theft must grapple with the frustration of having their privacy violated, their financial stability jeopardized, and their personal information continually exploited to commit further crimes, with astonishingly few resources available for assistance.[3]

It is often seen that the main defence used against the fake content is that an individual has freedom of speech and expression granted under Article 19 of the Constitution of India. The thing that is to be considered is that our freedom of expression ends where one's right to privacy begins. Our duty here is to understand that our actions and freedom does not tend to hamper any other individual's enjoyment of rights.[4] Freedom under Article 19 can't be used to justify the creation and dissemination of fabricated or altered videographic content/still image having capability to manipulate people's thought process regarding the subject of the content. Hence, to combat this, the regulators and citizens should do their duty towards the welfare of the public.[5]

The world has however started taking cognizance of the threat it possesses and this can be easily seen by several Countries looking forward to bringing this technology under their legal ambit. Regulating the big social media platforms is necessary so that they keep a check and balance on the fake content that is uploaded, shared and downloaded using their platforms that is capable of causing potential damages.[6] It needs to be brought under control, as in this digital world, Privacy and Identity matters more than ever and efforts need to be taken to prevent its breach. Same has been ensured by the Courts through its various judgments highlighting the need of special Laws and regulations to deal with the menace of Identity Theft committed through DeepFake and safeguarding Right to Personality.[7]

II. JUDICIAL APPROACH

Personal privacy in its most basic form, which is tied to the most intimate aspects of one's existence, is inextricably linked to the quality of one's life. Over the course of history, privacy has been associated with a variety of things, including private correspondence, family life, and one's own personal space. From the 14th to 21st century, a large number of people travelled to

[3] *Ibid.*
[4] Shashank Shekhar & Ashish Ransom, *Ethical & Legal Implications of Deep Fake Technology: A Global Overview,* 11 CIENCIA & ENGINEERING JOURNAL. 2233, (2023).
[5] *Ibid*.
[6] *Id.* at 2234.
[7] Ashish Jaiman, *The Danger of Deepfakes*, THE HINDU (Jun. 1, 2025, 12:00 PM), *https://www.thehindu.com/sci-tech/technology/the-danger-of-deepfakes/article66327991.ece*.

 [ISSN 2581-5369]

court in order to bring this right into existence and make it a reality.[8] The evolution of the Right to Privacy, culminating in its recognition under Article 21 of the Indian Constitution, is a journey marked by legal precedents, societal changes, and philosophical debates. Spanning centuries, this evolution reflects humanity's growing awareness of individual autonomy, dignity, and liberty in the face of technological advancements and expanding state power.

The concept of privacy, as we understand it today, finds its roots in ancient civilizations where individuals sought solitude and protection from unwanted intrusion. However, the formal recognition of privacy rights emerged much later in human history. One of the earliest legal frameworks to acknowledge privacy can be traced back to Roman law, where the concept of "dominium" recognized individuals' rights over their property, including their physical space and possessions. This notion laid the groundwork for modern conceptions of privacy as a fundamental human right.[9]

The Enlightenment era of the 17th and 18th centuries saw the proliferation of philosophical ideas emphasizing individual rights and freedoms. Thinkers like John Locke and Immanuel Kant articulated the importance of personal autonomy and the right to be free from unwarranted interference. These philosophical underpinnings provided intellectual justification for the recognition of privacy rights in subsequent legal systems.

The Industrial Revolution brought about significant societal changes, including urbanization and the rise of mass media. These developments raised concerns about the erosion of individual privacy as people increasingly found themselves subjected to surveillance and scrutiny. Legal responses to these challenges varied across different jurisdictions, with some enacting laws to protect privacy in specific contexts, such as communications and property rights.

In the United States, the right to privacy began to take shape in the late 19th century through a series of legal decisions and scholarly writings. One landmark case was Warren and Brandeis's "The Right to Privacy," published in 1890, which laid out a legal framework for protecting individuals from unwarranted intrusions into their private lives. This influential article argued that privacy is essential for maintaining personal autonomy and fostering social relationships.[10] The 20th century witnessed further advancements in privacy rights, particularly in response to technological innovations such as photography, telecommunications, and later, the internet. Legal frameworks adapted to address new challenges, with courts expanding the scope of

[8] Tom Head, *Where Did the Right to Privacy Come From?, ThoughtCo.* (May 6, 2025, 9:45 pm), *https://www.thoughtco.com/right-to-privacy-history-721174.*
[9] *Ibid.*
[10] *Ibid.*

 [ISSN 2581-5369]

privacy protections to encompass areas like personal information, medical records, and reproductive rights.

The concept of Right to Privacy has existed since the framing of the constitution even though the framers in the Constituent Assembly did not explicitly express it. Privacy rights were viewed as a basic human right, and not included in Chapter 3 of the Constitution, which lays down the fundamental rights. In India, the journey towards recognizing the right to privacy as a fundamental right under Article 21 of the Constitution was a gradual one, influenced by both domestic and international developments. The Constitution itself did not explicitly mention the right to privacy, but the Supreme Court began to interpret Article 21, which guarantees the right to life and personal liberty, expansively to include various facets of privacy.

Earlier there was nothing like privacy rights in Indian society and was denied in the case of *A.K. Gopalan v. State of Madras*[11] by giving a narrow interpretation of Art 21 of the Constitution. The Supreme Court of India, in its judgment, held that Article 21 only protects against arbitrary and unreasonable state action and does not guarantee absolute rights. The Court also held that the Preventive Detention Act was a valid law and did not violate the Constitution. The judgment was criticized for its narrow interpretation of fundamental rights and for upholding the validity of preventive detention laws, which were widely used by the government to suppress dissent. The case had significant implications for the protection of civil liberties and human rights in India. It sparked a debate about the need for judicial review of state action and the role of the judiciary in protecting the fundamental rights of citizens. The judgment was seen as a setback for civil liberties activists, who argued that the state's power to detain citizens without trial was a violation of basic human rights.[12]

Similarly, in *M P Sharma v. Satish Chandra*[13], Right to Privacy was discussed and the court ruled that the authority to search and seize was the highest priority of the state which needed to protect society. It was noted that the authority to search and seize could not be subject to the right to privacy, as the Constitution of India did not have a provision prohibiting unjustified search and seizure equivalent to Article 4 of the Amendment to the US Constitution. Therefore, the court upheld the government's right to search and seize.[14]

---

[11] AIR 1950 SC 27.

[12]Jaya Sharma, *Case Commentary on A.K. Gopalan v. State of Madras,* ILEDU (June 1, 2025, 7:55 pm) *https://iledu.in/case-commentary-on-a-k-gopalan-vs-state-of-madras/.*

[13] AIR 1954 SC 300.

[14]Shreyansh Prakash, *M.P. Sharma vs Satish Chandra Case,* LEGAL LORE (May 30, 2025, 7:35 pm) *https://www.legallore.info/post/m-p-sharma-vs-satish-chandra-case* .

 [ISSN 2581-5369]

One pivotal moment came in *Kharak Singh v. State of Uttar Pradesh*[15], where the Supreme Court recognized the right to privacy as an intrinsic part of personal liberty under Article 21. This case involved the legality of police surveillance on individuals' movements, and while the Court upheld the surveillance measures, it acknowledged the importance of privacy in safeguarding individual freedom.[16]

In *Govind v. State of Madhya Pradesh*[17], it was held that the right to privacy is not explicitly stated in the Constitution and assumed that though it emanates from the right to liberty, the right to move freely, and the right to speech, it cannot be an absolute right and should be subjected to the compelling public interest. The law infringing the right to privacy must satisfy compelling state interests.

In the State *of Maharashtra & Ors. v. Madhukar Narayan Mardikar*[18], the Supreme Court held that even a woman of "easy virtue" has the right to protect her privacy, and it would not be open to any person to violate her private space at his whims. The court further disagreed with the Bombay High Court's assessment, which dismissed the testimony of the lady on the grounds that she was an unchaste woman and her testimony could not be believed to ruin the career of a public official. It was held that even a woman of easy virtue enjoys the right to privacy and is entitled to the protection of the same.

In *R. Rajagopal v. State of Tamil Nadu*[19], also famously known as the Auto Shanker Case, the Right to Privacy was dealt with against the right of the media to publish the autobiography of a prisoner exercising the right to freedom of speech and expression under Article 19(1)(a). The Supreme Court held that the publication of a person's life story without his consent is violative of his right to privacy, and the person is entitled to damages for injuries resulting from an unauthorised invasion. The right to privacy, though not explicitly mentioned in the Constitution of India, is the penumbra of the right to life and personal liberty under Article 21. The right to privacy entails the right to be let alone.

PUCL v. Union of India[20], was the first PIL case to challenge the constitutionality of a law as violative of the right to privacy. The Civil Society Organisation People's Union for Civil Liberties filed a petition in the Supreme Court contending that Section 5(2) of the Indian

[15] 1964 SCR (1) 332.
[16] Shivani Kumari, *Right to Privacy,* IPLEADERS BLOG (June 1, 2024, 11:50 PM), *https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/#Govind_v_State_of_Madhya_Pradesh_1975* (last visited June 1, 2025).
[17] AIR 1975 SC 1378.
[18] AIR 1991 SC 207.
[19] 1994 SCC (6) 632.
[20] AIR 1997 SC 568.

 [ISSN 2581-5369]

Telegraph Act, 1885, gives the state executives the power to tap the phones of individuals in certain circumstances as a stark attack on the individual's privacy. The Apex Court held that the right to privacy is guaranteed under Article 21 of the Constitution by referring to the previous judgements in MP Sharma's case, Kharak Singh's case, Gobind v. State of M.P., and Rajagopal's case. The right to have a telephonic conversation without intrusion is a part of the right to privacy under Article 21 and cannot be curtailed except by procedures established by law.

In the instances of cases of Gobind, PUCL telephone tapping, and R. Rajagopal, the Indian Constitution recognised privacy as a basic right. Despite three distinct judgements by smaller benches in India's Apex court, the parties involved are still confused about whether Article 21 of the Indian Constitution incorporates privacy safeguards or not. The Apex court concluded that the right to privacy is a constitutional right and that a tort action for damages for an illegal violation of privacy is one component of the right to privacy. The right to privacy is protected as a constitutional right, not as a civil right.

However, it wasn't until the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[21], that the Supreme Court explicitly recognized the right to privacy as a fundamental right under Article 21. In this case, the Court held that privacy is an essential aspect of human dignity and autonomy, integral to the exercise of other fundamental rights. The judgment marked a significant milestone in India's legal history, affirming the right to privacy as a cornerstone of individual liberty and limiting the state's ability to intrude into citizens' private lives without just cause. Since then, the Court has continued to refine its understanding of privacy rights, balancing them against competing interests such as national security and public welfare.

Thus, the evolution of the right to privacy from its nascent roots to its recognition under Article 21 of the Indian Constitution reflects a broader global trend towards acknowledging the importance of individual autonomy and dignity in an increasingly interconnected world. The right of privacy is considered as a fundamental right of the individuals in almost all the countries of the world. The availability of the data in the cyber space, through hacking or by other means with capability to access, may cause the criminal infringement of privacy. It also causes the infringement of the right of privacy enshrined in Article 21 of Constitution of India. The Hon'ble Supreme Court has categorically ruled that the right of life includes the right of privacy as well. According to Article 12 of the United Nations Declaration of Human Right also, every individual has a right to privacy.

[21] (2017) 10 SCC 1.

 [ISSN 2581-5369]

Privacy in cyberspace, is thus, the right to choice as to who can contact or observe us and to control how our personal information is collected, used, and shared. Posting personal photos or innermost thoughts online is a choice, but one should also be able to choose with whom one is sharing that personal information, whether it's other individuals, advertisers, or organizations. Privacy is a way to protect oneself and family from identity theft and fraud that can threaten the financial, emotional, and even physical well-being. However, in this digital world, privacy of a person is under constant threat due to easily accessible personal information for the cyber criminals that could be used to commit Identity Theft. Person's private information is fodder for fraudsters. Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion.[22]

A single company may possess the personal information of millions of customers. It needs to be kept private so that customers' identities stay safe and protected and the company's reputation remains untarnished. Data privacy ensures that individuals are in control of how their personal information is collected, managed, and shared by companies that have access to it. Data privacy refers to the handling of critical personal information, also known as personally identifiable information (PII) and personal health information (PHI). Fair Information Practice Principles given by the Organization for Economic Cooperation and Development (OECD), have become an informal standard for how organizations should handle personal data. They are widely echoed in many privacy frameworks, including GDPR and the CCPA.

The eight principles are as follows-

1. Collection limitation: Personal data collection should have limits.
2. Data quality: Personal data must be accurate and relevant to its intended purpose.
3. Purpose specification: The purpose of collecting personal data must be explicitly stated.
4. Use limitation: Personal data should not be used for purposes other than the stated purpose.
5. Security safeguards: Personal data must be kept secure.
6. Openness: Individuals should be informed about the collection and use of their personal data.
7. Individual participation: Individuals have the right to access their personal data, to have it corrected or erased, and to know who has access to it.

[22]IDX, *A Savvy Consumer's Guide to Privacy & Identity Theft,* IDX.US (May 19, 2025, 8:45 pm) *https://www.idx.us/knowledge-center/a-savvy-consumers-guide-to-privacy-identity-theft*.

 [ISSN 2581-5369]

8. Accountability: Those who collect personal data must be responsible for following these principles.

These rules prevent data from falling into the wrong hands. It's everyone's legal right to regulate the manner in which, when, and to what degree their personal data is shared with others. Identity theft by way of deepfakes poses a constant threat as it violates Right to Privacy under Article 21.

The Right to Privacy was, with time, extended to include Right to Identity as a part of Art 21. The Constitution of India recognises the importance and protects the dignity of personal identity of its citizens most emphatically under Article 21. The sum total of rights and duties that one enjoys as a person, in various walks of life, is what constitutes one's personality in law. And Personal Identity, therefore, is one's unique personality under the law. The defamation of a person, which means harming the reputation, is something that has a tendency to adversely affect one's personal identity.[23] In *Pragati Shrivastava v. CBSE*[24], SC held that "a name is an identity marker, and that the right to be identified by one's name, and also as the daughter or son of parents whose name is correctly mentioned, is fundamental to one's very identity as an individual."

On the Internet anyone can get such an identity in more than one way. Not only this, one can easily get an identity in the name of others in an unauthorised manner and use it to the detriment of the person concerned; or can create a fake identity and use it to commit several offences in the cyber world. Most interesting feature of personal identities in the cyber world is nowadays playing great roles in molding the opinion of the masses. However, people are creating fake identities and operating the same to take part in various opinion polls. Such identities are being created either in the name of living persons (like that of A B Bajpayi) or persons dead and gone long since (like Subhash Chandra Bose) or by any other name in which case it is only a fake personal identity and any similarity with the name of some living person is only a coincidence which cannot be taken to represent that other person's opinion even if it is akin to the opinion of that other person. Thanks to such fake personal identities, succeed in giving desired signals to the masses. Before the true picture is known, if it is known at all, much damage has been done.[25]We must sensitize the public about the existence of such a technology on the one hand. We must teach the youth not to blindly trust any news or video we see on social media unless

[23] J.P. Mishra, *Personal Identity and Law*, 2 INTERNATIONAL JOURNAL & LEGAL JURIS. STUDIES. 5, (2015).
[24] 2024 SCC OnLine Del 2688.
[25] *Ibid*.

 [ISSN 2581-5369]

it is coming from an authentic source or is verified by an authentic source. On the other hand, we must bear in mind that our right to freedom of expression ends where it starts infringing upon the right to privacy of other individuals.[26] The critically minded and informed citizen is key to democracy, more so in these times of generative AI. Neither disinformation nor deep-fakes are a technological problem, these are socio-political problems and ought to be treated that way.[27]

III. ISSUES WITH A BLANKET BAN ON DEEPFAKE

When it comes to technological tools, outrightly imposing a blanket ban on particular activities is never the best solution. Instead, it is through effective regulatory measures that the socio-legal issues can be tackled most efficiently. In the case of deepfake technology and its usage, there are three extremely significant considerations which are convincing enough against a complete ban, namely –

1. Firstly, it is highly difficult to distinguish between original content and deepfake content. As a result, detection becomes close to impossible. Unless detected, any legal measure banning deepfakes wouldn't be fully operational and effective;
2. Secondly, a complete ban on deepfake content would be violative of the freedom of expression of individuals at large. Article 19 of the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR) provide for the right to freedom of expression to individuals globally;
3. Thirdly, like any other tool, deepfake technology is not causing harm in all cases, but rather it has proven to have beneficial utility in some situations. It plays a key role in routine modifications thereby improving the overall clarity of content on the digital platforms.[28]

Nowadays, audio-visual deepfakes involving lip-syncing can be created, thereby allowing the conversion of advertisements and other videos in different languages without the efforts of re-shooting several times. For instance, David Beckham's announcement for the 'Malaria Must Die campaign' was created in nine different languages using deepfake technology to increase the reach of the message. This is a perfect example to show that deepfakes have made the issue

[26]NISHA DHANRAJ DEWANI, HANDBOOK OF RESEARCH ON CYBER LAW, DATA PROTECTION AND PRIVACY 47 (2022).
[27]Anirban Bhaumik, *Disinformation, deepfakes are socio-political, not technological, problem,* DECCAN HERALD (Mar. 8, 2024, 10:30 pm) *https://www.deccanherald.com/elections/india/battle-of-ballots-in-the-age-of-ai-2928842.*
[28] NISHA DHANRAJ, *loc.cit*.

 [ISSN 2581-5369]

of bad dubbing and language barriers a thing of the past with its high quality real looking content creation skill. Furthermore, deepfakes can be used as a double-edged sword to give the video gamers and movie audience an excellent experience by providing a platform for the creation of videos and video games with high quality VFX technology at an accelerated speed and pocket-friendly costs. By democratizing the extremely costly VFX technology in this manner, deepfakes can make it a win-win situation for both the creators and the audience.

Another advantage of deepfakes is that it can allow the viewers to experience watching and interacting with famous fictional or dead personalities as if they were alive. The entertainment and cultural industry can flourish by the usage of deepfakes as happened in the Dali Museum, Florida wherein people brought the famous Spanish artist Salvador Dali back to life with the help of deepfake technology and allowed the museum visitors to watch, interact and click pictures with the long-gone famous artist. Similarly, Mona Lisa was also brought to life using this AI-generated synthetic technology in Samsung AI laboratory, Moscow, thereby astonishing the visitors. For the same reasons, no country has imposed a complete legal ban on deepfakes yet.[29]

IV. Conclusion

Identity theft can have devastating financial implications for victims. Addressing the impact of identity theft on the right to privacy requires a multifaceted approach. Effective cybersecurity measures, such as encryption, authentication protocols, and robust data protection laws, are essential for safeguarding individuals' personal information against unauthorized access and misuse. Moreover, increased awareness and education about the risks of identity theft can empower individuals to protect themselves and mitigate potential harm. Identity theft poses a significant threat to individuals' right to privacy, with far-reaching implications for financial security, emotional well-being, and societal trust. As technology continues to evolve, addressing the complex challenges posed by identity theft will require concerted efforts from governments, businesses, and individuals alike to ensure that privacy rights are upheld and protected in an increasingly digital world.

As per International Association of Privacy Professionals (IAPP), Privacy is possible in the digital age. It just takes some knowledge and effort in this digital world. With knowledge and preparation, one could protect what's personal and share information with confidence. One may be an introvert or an extrovert, a couch-surfing hermit or an outgoing party animal. But in today’s world, data privacy isn’t just a personal preference. It’s a matter of personal safety.

[29] *Ibid.*

 [ISSN 2581-5369]

Privacy is a "right to be left alone", that is an extension of liberty, and anyone who uses another person's identity without that person's consent is seen to have violated both that person's personality rights and their fundamental right to privacy.[30]

*****

[30] *Ibid*.

 [ISSN 2581-5369]