



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

IDENTITY GAP

BY PRIYANKA KHAWALE

ABSTRACT

The technological evolution has reshaped the routine life of an individual, today a person's social standing is determined based on how influential a person is on the digital and social media platforms. This shift has underlined a direct bearing on the law of digital identity theft because it changes what identity actually consists of. A person's digital identity is no longer just their name, password or biometric but it now includes their voice, face, mannerisms and online persona, all of which are now digitally reproducible with advancement of artificial intelligence.

INTRODUCTION

A digital identity is the combination of information about a particular individual that exists online. One's digital identity includes anything online that is associated with their name such as social media posts, interactions, articles, publications, institutional affiliations and more. Our digital identities are created by how we present ourselves and how we are seen by others in both personal and professional settings. But why is understanding digital identity important? Who we are online gives others insight into who we are in real life, this leads us to make assumptions about people even if we have never met them in person.

In digital identity, authenticity is important. What we see online does not always reflect how a person is in the real world. One needs to understand that a digital identity is a curated image of a person that may not always reflect their whole self. The online world can even contain false identities that differ drastically from who the people behind them really are. And such false identities fall under the bracket of Digital Identity Theft.

In simple language, identity theft is a fraud or a deception perpetrated by the person who is the perpetrator of the crime in which he or she accesses sensitive information of the victim and then utilizes this information to his or her advantage.

TYPES OF IDENTITY THEFT

The first is financial identity theft. A prominent identity theft observed in India post pandemic, here the fraudster accesses information pertaining to the credit card or the bank of the victim through calls, messages or emails and then uses it to make online purchases or to access the bank account and take out money without the consent or knowledge of the victim. This financial identity theft was observed to have various other factors involved such as digital arrest, issuance of warrant or even the prevalent one included mentioning of illegal substances being delivered on their address if not paid the amount. The victims initially were digitally vulnerable people.

The second kind is social identity theft. This kind of identity theft is usually observed on social media platforms, here the person's information on the social media such as the name, the address, the photograph, videos, etc. are accessed by the fraudster or third-party and then utilized it either to impersonate the person or to or to use the person's identity for some act which would be illegal or criminal. Many adolescents out of vengeance also tend to commit this cyber crime without realizing its consequences.

The last type of identity theft is known as synthetic identity theft. In synthetic identity theft, it usually includes original personal data which is collected by the fraudster from the financial sector or some information from social media, utilizing this information with fake details to commit a fraud, such as a loan in the name of the person by using his details and then defaulting on the loan or generating credits on infants name or availing credit cards.

The preventive measures for such crimes are awareness and digital literacy. India has already implemented it by setting a mandatory caller tune of awareness message in all languages in order to digitally literate people of the guidelines, the crimes as well as clarify the basic understanding of concepts. This is likely to reduce such cyber crimes and help implementation of better legal enforcements.

IDENTITY THEFT VS IDENTITY FRAUD

Let's understand the distinction between identity theft and identity fraud with a daily life example.

For instance, Priya and Smita have always been archenemies, one fine day Smita out of vengeance makes a profile with the username as Priya and also puts up a profile picture obtained through Priya's genuine social media account without her consent. This act amounts to digital identity theft as Smita has illegally acquired Priya's personal data and set up a false account without Priya's knowledge. Digital Identity Theft is said to be the initial step of digital identity fraud. Digital identity theft is illegal acquiring of someone's personal data without their consent.

Now in the same above scenario if Smita out of vengeance uses this fake profile to deceive Priya's friends, or posts, messages tarnishing Priya's reputation with an intent of fraud and deception. Then it would amount to digital identity fraud. As she has caused harm and is using the identity to deceive others. Digital Identity Fraud is an umbrella term which includes cyber crimes such as phishing, impersonation, deepfakes or catfishing. The most prevalent kinds of digital identity frauds recognized globally as well as in India are currently phishing attacks including fraudulent mails, links and false credentials and online financial frauds.

THE STATUTORY LACUNA

India lays down two extensive acts to regulate laws specifically dedicated to technology and privacy with reference to the apprehension of emerging cyber crimes. During the era of the [Information Technology Act, 2000](#) many of the provisions mandated were future sighted, not only did the legislation but also the judicial interpretations enhanced the concept of cyber crimes and working of technology with the anticipation of its misuse.

This statutory framework also overlaps with the provisions of [Bhartiya Nyaya Sanhita, 2023](#), previously [Indian Penal Code 1860](#) for crimes such as cheating and forgery. It overlaps with [Bhartiya Nagarik Suraksha Sanhita, 2023](#), previously [Code of Criminal Procedure, 1973](#) which lays down the administrative and investigative framework while addressing the procedure for seizure and e-FIR for digital identity theft. Overlapping with [Bhartiya Sakshya Adhiniyim, 2023](#), previously [Indian Evidence Act, 1872](#) in evidentiary capacity by defining the crime and its punishment.

In the year of 2017, when a grave issue arose before the Hon'ble Supreme Court of India, the judicial interpretation laid down a landmark judgement that later became the foundation of the [Digital Personal Data Protection Act, 2023](#). "Privacy", a concept on which all the laws remained silent even in the digital era of [IT Act, 2000](#), gained a definite space under [Article 21 of the Indian Constitution](#). The Right to Privacy was no longer a myth but a fundamental right of the citizens.

Now with the emerging technology trends, another fear arises of the advanced functioning of artificial intelligence which is undistinguishably accurate. Our laws, although far sighted, remain unaddressed to the emerging crimes occurring with the use of Artificial Intelligence. The above mention of landmark judgement in the case of [Justice K.S. Puttaswamy v. Union of India, 2017](#) underscores that the modern judiciary not only applies laws as they are, but actively interpret them to shape societal needs. One such interpretation is necessary in terms of rising digital identity thefts.

LEGAL FRAMEWORK

The legal provisions in India are derived from the dedicated legislation and judicial interpretations which address situations where the identity is stolen and not when fabricated. [*Section 66C of the Information Technology Act, 2000*](#) was framed for a particular kind of crime. It penalizes digital identity theft when someone fraudulently or dishonestly steals or uses your password, signature, or other unique identification feature. The provision assumes the identifier being misused was taken without your permission.

Artificial intelligence breaks this assumption entirely. A voice-cloning tool does not steal your voice. It listens to a few seconds of you speaking pulled from a phone call, an Instagram reel, a YouTube interview and builds something new which is a synthetic reconstruction that sounds like you but was never technically yours. Here nothing is taken yet something is manufactured. And this is precisely where the difficulty lies, because *Section 66C* addresses "unique identification feature" as a fixed, singular thing attached to a person. A deepfake is not that. It is closer to a forgery of a person's entire presence than the theft of any single feature belonging to them.

[*Section 66D of the Information Technology Act, 2000*](#) penalizes cheating by impersonation using a computer resource and pretending to be someone else through a computer network in order to deceive or defraud. The provision throws light on scenarios like fake profiles and phishing, where an individual is extorted of money or information because someone convincingly pretended to be someone else. AI voice-cloning scams targeting families are a case in point, and reports of them have grown steadily. For instance, a fraudulent caller uses a synthetic voice mimicking a relative in distress, urgently asking for money or in the prevalent scenarios observed, the caller impersonating to be a police officer extorting money by threatening with the concept of digital arrest. Usually in the above described scenarios, the victim does not hand over money because their password was compromised but they pay because they were deceived by someone who sounded unmistakably like someone they trusted, or an authority they feared.

Under the [*Digital Personal Data Protection Act, 2023*](#) although no such provisions exclusively address digital identity theft or any third-party fraudsters activity, yet it regulates data fiduciary provisions to protect what an individual holds. The General Obligation of Data Fiduciary is mentioned in the [*Section 8 of the Digital Personal Data Protection Act, 2023*](#) that requires the fiduciaries or data handlers to take reasonable safeguards to prevent personal data breaches. Certain duties of the Data Principal are also expressed under [*Section 15 of the Digital Personal Data Protection Act, 2023*](#), it explicitly states that an individual must not impersonate another while providing personal data for any document or unique identification.

It leaves a blind spot in the legal statutory framework. The law protects credentials from theft, and regulates how fiduciaries deal with data, yet remains silent on the fabrications of a persona from the data that was never stolen, often because it is already public.

JUDICIAL INTERPRETATION

1. [*Anil Kapoor v. Simply Life India & Ors. \(2023\)*](#) decided by the Hon'ble Delhi High Court addressed the emerging issue against misuse of generative artificial intelligence, deepfakes and digital identity theft.

The infamous actor Anil Kapoor had filed a lawsuit against 16 platforms who were using his publicly recognizable identity without his consent through generated deepfakes, morphed pictures, cloned voice in the form of ringtone and merchandise with catchphrase “*Jhakaas!*” for promotion of their goods.

The Hon'ble Delhi High Court passed an ex parte interim injunction restraining use of Anil Kapoor's name, image or voice for any financial gain. The court had directed blocking of such deceptive links as well as domain names with malicious content.

2. [*Arijit Singh v. Codible Ventures LLP & Ors. \(2024\)*](#) decided by the Hon'ble Bombay High Court was the first judicial intervention in the music industry and generative AI voice-cloning.

The famous playback singer Arijit Singh filed a suit before the court after discovering several platforms using Real Voice Cloning (RVC) technology. These platforms not only sold access to the software which could clone any audio file to a performance sung by Arijit Singh but also had a step by step guide to bypass license restrictions. These cloned audios gained popularity creating content for event promotion and illusion of endorsements.

The Hon'ble Bombay High Court passed an ex parte interim injunction against violation of singer's fundamental publicity and personality rights. The generated contents were taken down as mass scaling directly threatened the artist's livelihood.

INTERNATIONAL FRAMEWORK

The European Union's [*General Data Protection Regulation \(GDPR\)*](#) is a statutory framework implemented and mandated by the European Union with effect on 25th May, 2018. It has also laid down a strong foundational base to interpret data privacy laws. GDPR introduced various safeguards in order to secure personal data. The legal safeguards mandated through enforcement included consent driven access of personal data and limited purpose with exact reason before collection to be disclosed. India has adopted its [*Digital Personal Data Protection Act, 2023*](#) and [*Digital Protection Data Privacy Rules, 2025*](#) through the understanding of [*General Data Protection Regulation*](#).

An extensive comparative analysis of the [Digital Personal Data Protection Act, 2023](#) and [General Data Protection Regulation](#) concludes that

- GDPR contains stricter preventive measures and standards for special data categories that includes biometrics or national ID numbers since it addresses both digital as well as physical data, DPDP Act, 2023 contains a broader application since it focuses more on digital personal data.
- The DPDP Act is more consent driven as it introduces data intermediaries (consent managers) to manage digital consents on behalf of the data principal whereas in GDPR either the consent is managed by the user or through settings of automated systems.
- Unlike the Indian framework, GDPR provides pre-emptive claims for emotional distress even before actual misuse happens, it also regulates rights explicitly to sue the companies for victims financial and emotional compensation.
- The DPDP Act has an immediate breach notification mandating to the users as well as the Data Protection Board regardless of the loss and risk level whereas GDPR has a conditional framework of reporting within 72 hours to the regulators.
- Under the DPDP Act, the law fines Data Principals for frivolous reporting, submission of deceptive documents or impersonation. GDPR lacks to formulate such a provision against mistaken breach grievances or incorrect filing.
- Unlike DPDP Act's framework, under GDPR the burden of proof lies on an individual to prove the company's failure or breach in security safeguards which has caused them damage or loss of control.

RECOMMENDATIONS

The first step is definitional. Digital identity theft, as it stands under [Section 66C of the Information Technology Act, 2000](#), has been given a fairly narrow reading that is limited to the dishonest use or theft of a password or other unique identification feature. That definition needs to widen alongside the evolving capabilities of artificial intelligence. The adaptable solution is either introduction of a provision or an AI-centred legislation that identifies the specific activities and degrees of AI misuse that ought to be criminalised. The offence should turn on deceptive intent and the act of fabrication itself, not on proving that something was stolen.

Secondly, although the [DPDP Act](#) mandates for digital privacy of an individual and regulates relationship between the Data Principals (users) and Data Fiduciary (companies), the question of accessible pictures or videos of an individual publicly to any fraudsters or third-party without the consent of the Data Principal makes it easier to build a deepfake. For instance, without any

breach, pictures of you are available online on your choice of social media accounts, a stranger rather than stealing just builds a fake version of you through use of the photos you have posted. The Act does not regulate or penalize such activities yet as it addresses relationships between fiduciaries and principals and no third party relations are mentioned. Here, the Act should provide safeguards to the victims to act even when there's no data fiduciary involved.

Thirdly, a small yet necessary step of the users which may safeguard their own personal data is Multi-Factor Authentication (MFA). Although MFA serves as a safeguard against major cyber crimes such as digital identity fraud, it may not protect from cloning a digital identity. Multi-Factor Authentication requires the user to provide two or more distinct facts to verify their identity before granting any access to a system or an account. It is to ensure security from hackers or safeguard from fraudsters from obtaining any information through the internet. MFA works on a three-tier system. The verification on tier one includes a password or a pin or any kind of secret code or a question, tier two includes possession of the device - a mobile phone receiving notification which serves as the token generator and lastly, tier three contains biometric data which is unique and it works as a strenuous pass. Biometric data may include fingerprints, facial recognition or even retina patterns. MFA reduces the risk of threat to the data while safeguarding the core.

CONCLUSION

The newspaper headlines often have one article in bold either regarding “digital arrest” or “online financial frauds”. If one reads closely one would notice the pattern in detail that in these scenarios, victims of such crimes are not hacked but convinced. A familiar voice on call or an officer on a video call claiming to digitally confine you in your own house are the results of fear as a stigma and digital unawareness. The safeguards provided under well defined provision of the [*Information Technology Act, 2000*](#) and [*Digital Personal Data Protection Act, 2023*](#) protect citizens against theft of password or other unique features, penalizes impersonation while the DPDP Act, 2023 exclusively governs fiduciaries hold on the personal data, their collection methods and storing while ensuring necessary security safeguards. These dedicated legislation cover the whole yet nothing in these provisions currently address fabrication of persona as a wrong itself.

Filling in such a lacuna in the laws, the judiciary steps in with the apt interpretations necessary for the need of hour. The Hon’ble Courts based on circumstances of the case, issues raised and arguments made fill this gap. The judgments passed in Anil Kapoor's and Arijit Singh's case lay down as a precedent and landmark to regulate interpretation of existing laws to safeguard one's persona. Thus, we may infer, if famous personalities face a severe issue of being cloned, even an ordinary person's voice can be cloned, image can be morphed through a single post, video or reel available and accessible on social media platforms.

The basic recommendations as stated above begin with widening the definition not only through judicial interpretation but also through amendments. Till India enacts an artificial intelligence dedicated legislation, the existing provisions need to safeguard the victims and

penalize the perpetrator. The digital identity in the new provision not only needs to address the meaning extensively but also underline the misuse of artificial intelligence and its degree of application.

A person today heavily relies on his social standing determined by his digital presence. Our laws need to protect this particular presence in the same manner as the current laws protect a password or digital signatures. Until then, every digital identity is under the threat of being cloned faster than being defended.