



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.

From Life to Legacy: The Unsettled Question of Privacy After Death

Shanvi Mohanty^a Mini Sharma^b

^aMaharaja Agrasen Institute of Management Studies, Delhi, India ^bMaharaja Agrasen Institute of Management Studies, Delhi, India

Received 16 June 2026; Accepted 16 July 2026; Published 20 July 2026

In the present digital age, death no longer marks the end of an individual's societal presence. The rapid expansion of digital technologies has transformed the way individuals create, store, and share personal data, resulting in digital footprints that persist long after death. Social media accounts, emails, cloud storage, and other digital assets raise acute questions regarding ownership, access, consent, and the protection of the deceased person's dignity. The most pressing question is whether deceased persons remain protected with respect to their private data, or whether their digital privacy can be exploited with impunity. Currently, legal frameworks treat privacy as a right that extinguishes upon death, leaving significant gaps in protection. This article examines posthumous privacy through the lens of Indian constitutional principles, judicial precedents, and the existing legislative framework. It further explores emerging challenges posed by digital inheritance, artificial intelligence-driven recreations of deceased individuals, deepfakes, digital avatars, and other AI technologies. Drawing on comparative insights from Germany and the European Union, the article argues that the absence of a clear legal framework governing privacy after death necessitates a comprehensive legislative response that safeguards dignity while balancing the interests of surviving family members and the pace of technological innovation.

Keywords: *posthumous privacy, digital legacy, digital inheritance, personality rights.*

INTRODUCTION

A digital footprint is the trail of information created by an individual's activity online. It encompasses data intentionally published, such as social media posts or account registrations, as well as information collected automatically through websites and tracking technologies. Every interaction with a connected device contributes to detailed profiles built by organisations, corporations, and, increasingly, by cybercriminals: location data, browsing patterns, online purchases, and public Wi-Fi network connections are among the constituent elements of this ever-growing digital portrait. These profiles are monetised by companies for targeted advertising, leveraged by employers for background verification, and, critically, they persist after the individual who generated them has died.

Post-mortem privacy refers to a person's ability to control the dissemination of their personal information after death, including the protection of their reputation and dignity. In India, no specific legal framework explicitly extends post-mortem privacy protection to deceased individuals. The position remains deeply ambiguous under the Digital Personal Data Protection Act, 2023 (DPDPA).¹ The absence of such recognition has generated increasing controversy, given that technological advancement has dramatically expanded the volume of private information stored and shared online. Medical confidentiality constitutes a limited exception under the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulation, 2002.² Digital assets present unresolved questions under the Information Technology Act, 2000,³ while service providers' terms of service agreements remain the closest variant to practical guidance, with platforms such as WhatsApp permitting legacy contact access only if pre-designated, and Google requiring court orders, death certificates, and legal heir documentation before granting access to deceased accounts.

The fundamental issue in posthumous privacy discourse is deceptively straightforward but profoundly significant: does an individual's right to privacy cease with their death? In the current digital era, individuals leave behind not only tangible possessions but also emails, social media profiles, photographs, messages, and substantial personal data. New technologies such as artificial intelligence can now replicate a deceased person's voice,

¹ Digital Personal Data Protection Act 2023

² Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulation 2002

³ Information Technology Act 2000

likeness, or even personality, introducing fresh concerns regarding consent and dignity after death. While extending privacy rights beyond death could honour the deceased's wishes and legacy, such extension must be weighed against freedom of expression, public access to information, and the rights of surviving relatives. The true challenge lies not merely in deciding whether privacy should persist after death, but in determining the scope of such protections and identifying who should be entrusted with their enforcement.

UNDERSTANDING POSTHUMOUS PRIVACY

Privacy, in its most fundamental sense, refers to the condition of personal and informational seclusion, the assurance that what is intimate remains so. In India, the right to privacy has emerged as a cornerstone of individual freedom, dignity, and autonomy. Posthumous privacy extends this concept to protect a person's reputation, secrets, moral values, dignity, and digital holdings after their death. The weight accorded to a deceased individual's private data and public image has become a defining issue of the digital age.

The tension between posthumous privacy and family interests has become particularly acute in India's emerging digital inheritance landscape. In the landmark ruling of *Sadhna Shaishav Shah & Anr. v Apple Distribution International Ltd.*, 2026, the Court of the 3rd Additional Senior Civil Judge, Gandhinagar, held that the right to privacy does not survive death and is not inheritable by legal heirs.⁴ Despite this holding, the court simultaneously granted the deceased man's daughter access to his iPhone and iCloud account by issuing a Letter of Administration over the digital estate, determining that digital data may form part of a deceased person's estate under the Indian Succession Act, 1925.⁵ This pragmatic approach prioritises the family's right to inherit and manage the deceased's assets over any abstract notion of continued posthumous privacy rights. However, the decision creates an internal tension: if digital data is property capable of succession, can it simultaneously be stripped of the privacy protections that constituted its very character during the owner's lifetime?

This tension reveals a fundamental conflict between two competing interests. On the one hand, surviving family members have legitimate interests in accessing the deceased's emails, photographs, financial records, and other digital content for administrative purposes,

⁴ *Sadhna Shaishav Shah v NIL* (2026) SCC OnLine Dis Crt (Guj) 1

⁵ Indian Succession Act 1925

emotional closure, or the preservation of memories. On the other hand, the deceased may have intended to keep certain information private even from their closest relatives, and respecting that wish would require recognising some form of posthumous right to privacy. The Delhi High Court reinforced the mainstream position in *Krishna Kishore Singh v Sarla A. Saraogi*, 2021,⁶ and *Ruba Ahmed v Hansal Mehta*, 2021,⁷ holding that privacy is not inherent. The judicial tendency thus far is to treat digital data as inheritable property rather than as protected personal information deserving posthumous shelter.

The traditional legal maxim *actio personalis moritur cum persona*, a personal right dies with the person, predates the digital era entirely. It offers no meaningful account of digital data that remains accessible, monetisable, and reanimatable through artificial intelligence long after the person who generated it has died. Corporations increasingly exploit the data of deceased persons with scant regulatory safeguards: it is used for targeted advertising, algorithmic training, and the creation of digital avatars of deceased performers and loved ones. The law has not kept pace.

COMPARATIVE PERSPECTIVES: GERMANY AND THE EUROPEAN UNION

A comparative lens strengthens the case for reform. German law recognises a doctrine of postmortal *Persönlichkeitsrechte*, or posthumous personality rights, which persist for 30 years after death. Under this doctrine, the surviving relatives of a deceased person may bring actions to protect their memory and dignity, including against unauthorised commercial exploitation of their image or likeness. The Federal Court of Justice has consistently upheld that the dignity of the deceased, rooted in the constitutional guarantee of human dignity under Article 1(1) of the Basic Law, does not evaporate upon death. This reflects a philosophical commitment to personhood that Indian constitutional jurisprudence, with its own strong dignity-based foundation in Article 21, could productively adopt.

The European Union's General Data Protection Regulation (GDPR) takes a more cautious approach: it expressly excludes deceased persons from its scope, leaving member states to legislate independently.⁸ Several member states, including France, Italy, and Spain, have enacted specific national rules extending data protection to deceased persons for varying

⁶ *Krishna Kishore Singh v Sarla A Saraogi and Ors* 2021:DHC:1870

⁷ *Ruba Ahmed and Anr v Hansal Mehta and Ors* 2022: DHC:4263

⁸ General Data Protection Regulation 2016

periods. France, for instance, permits individuals to issue posthumous instructions regarding their personal data, which data processors must respect. This legislative variety demonstrates that there is no single correct answer, but there is a clear acknowledgement across mature legal systems that the question must be answered explicitly rather than left to judicial improvisation.

India, by contrast, has left the question unaddressed in its primary data protection statute. The DPDPA 2023 is silent on the status of deceased persons as data subjects,⁹ and the gap is not merely academic: millions of accounts, digital wallets, and data repositories of deceased Indians are currently governed solely by the contractual terms of foreign technology companies, with no statutory floor of protection.

DOES THE FUNDAMENTAL RIGHT TO PRIVACY SURVIVE DEATH? JUDICIAL ANALYSIS

The right to privacy in India achieved its fullest constitutional articulation in Justice K.S. Puttaswamy v Union of India, 2017, where a nine-judge bench of the Supreme Court unanimously held that privacy is a fundamental right implicit in Article 21 of the Constitution.¹⁰ The Court recognised multiple dimensions of privacy, informational, decisional, and dignitary, and Justice Sanjay Kishan Kaul's concurring opinion elevated personality rights from a common law entitlement to a constitutional right, grounded in the individual's authority to control how their identity and likeness are used commercially. Whether this constitutional protection extends beyond death, however, remained unaddressed in Puttaswamy and has been tested only in the following cases.

In Deepa Jayakumar v A.L. Vijay & Others, 2021, the Madras High Court's Division Bench considered whether the niece and legal heir of a former Chief Minister could seek an injunction preventing the production of films and web series about the deceased without consent.¹¹ The court distinguished between the applicant's own privacy rights and any claimed posthumous privacy rights on behalf of the deceased. Balancing the applicant's interests against the respondents' right to freedom of expression, and noting the substantial investments already made in production, the court declined to grant an interim injunction

⁹ Digital Personal Data Protection Act 2023

¹⁰ *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1

¹¹ *Deepa Jayakumar v A L Vijay & Ors* (2021) SCC Online Mad 2642

and held that the right to privacy does not survive death and is not inheritable. A significant weakness in this reasoning is the court's failure to consider whether the creation of commercially motivated content about a deceased public figure is genuinely an exercise of freedom of expression or whether it is closer to commercial exploitation, warranting a distinct legal analysis.

In *Krishna Kishore Singh v Sarla A. Saraogi and Others*, 2021, the father of actor Sushant Singh Rajput sued for the restraint of a film titled 'Nyay: The Justice', produced without family consent.¹² The Delhi High Court held that rights to privacy, publicity, and personality terminate upon death and are not inheritable. It further observed that because the film drew only on publicly available media sources, no breach of rights had occurred. While the inclusion of a disclaimer was offered as a palliative, the case reveals a lacuna: the court did not engage with whether the family had any independent right to object to the commercial use of publicly available information about their deceased relative, distinct from any right inherited from the deceased.

In *Rajagopal v State of Tamil Nadu*, 1994, the Supreme Court held that a publisher has the right to publish an individual's life story so long as the information derives from public records, even without the subject's consent.¹³ However, the use of information not available in public records could violate the right to privacy and attract legal liability. This principle, which Puttaswamy later incorporated into constitutional doctrine, draws a durable line between public information and private information—a line that arguably should persist beyond death.

The 2026 ruling in *Sadhna Shaishav Shah* (discussed above) represents the most current judicial position, simultaneously denying the posthumous survival of the right to privacy while treating digital data as inheritable property.¹⁴ This doctrinal inconsistency—privacy dissolves at death, but the data that carries it survives as property—requires legislative resolution.

¹² *Krishna Kishore Singh v Sarla A Saraogi and Ors* 2021:DHC:1870

¹³ *R Rajagopal v State of Tamil Nadu* AIR 1995 SC 264

¹⁴ *Sadhna Shaishav Shah v NIL* (2026) SCC OnLine Dis Crt (Guj) 1

DIGITAL LEGACY AND THE OWNERSHIP OF DATA AFTER DEATH

When a person dies in the digital age, they leave behind a layered estate that the law has only partially mapped. Social media accounts contain personal communications and photographs that may carry both sentimental and commercial value. Email accounts function as authentication gateways to banking, insurance, and investment platforms. Cryptocurrency wallets, NFTs, Demat accounts, and digital subscription services represent assets of real financial significance, yet they are secured by private keys and passwords that may be irrecoverable without the cooperation of the deceased. Digital diaries, voice notes, and medical records carry intimate personal information that the deceased may never have wished to disclose.

India's current legislative landscape attempts to govern digital assets through three principal statutes, but none were designed with digital legacy in mind. Section 14 of the DPDPA 2023 empowers Data Principals to appoint nominees who may exercise data rights, including access, correction, and erasure, upon the principal's death or incapacity.¹⁵ This is a meaningful innovation, but its protection is contingent on prior nomination. Where no nomination exists, the DPDPA 2023 offers no protection to the deceased's data, leaving an enormous default gap for the majority of Indians who have not engaged in formal digital estate planning.

The Information Technology Act 2000 treats email accounts, social media profiles, and digital data broadly as movable property, under which legal heirs may, in principle, claim access upon furnishing appropriate documentation.¹⁶ However, the Act contains no specific provisions regarding digital legacy, the bequeathing of digital assets, or the management of digital estates under intestacy. The Indian Succession Act, 1925, and the Hindu Succession Act, 1956, were designed for a world of land, jewellery, and paper securities; they do not recognise digital assets as inheritable property and provide no procedure for their transfer, management, or closure.¹⁷

¹⁵ Digital Personal Data Protection Act 2023, s 14

¹⁶ Information Technology Act 2000

¹⁷ Indian Succession Act 1925; Hindu Succession Act 1956

The resulting legal vacuum generates three critical unresolved questions:

Who owns digital data after death? Courts have held that privacy rights extinguish upon death, but digital data itself may form part of a deceased person's estate under succession law, creating the doctrinal inconsistency noted above.

Can heirs access accounts without court intervention? Access depends entirely on the platform's terms of service, whether a nominee was designated under DPDPA Section 14, and, in the absence of nomination, whether heirs can obtain a Letter of Administration or equivalent court order, a process that can take months or years.¹⁸

What is the status of consent after death? The DPDPA 2023 does not cover deceased persons; the IT Act contains no posthumous consent provisions, and no statute addresses whether consent given during life survives for purposes of data processing after death.

The practical consequences are severe. Families unable to access digital assets quickly enough may suffer irreversible financial loss, particularly in respect of time-sensitive investments or cryptocurrency subject to price volatility. Simultaneously, millions of deceased persons face the risk of ghost identity theft and posthumous financial fraud, as their credentials and personal data remain in accessible form, ungoverned by effective legal protection. It is currently technology firms, not Parliament, that determine the rules.

THE RIGHT TO BE FORGOTTEN AND ITS POSTHUMOUS DIMENSIONS

The right to be forgotten, the right to demand de-indexing or erasure of personal information from digital platforms and search engines, adds a further dimension to the posthumous privacy debate. For living persons, this right is contested but increasingly recognised: the Delhi High Court and various regulators have grappled with requests to remove outdated or irrelevant information from search results. For deceased persons, the question becomes more complex. Who may invoke the right to be forgotten on behalf of the deceased? Can a family member seek the erasure of embarrassing or private digital content that the deceased would have wished removed? Does the right to be forgotten survive death at all?

¹⁸ Digital Personal Data Protection Act 2023, s 14

Indian law currently offers no clear answer. The DPDPA 2023, which includes a right of erasure for living Data Principals, does not extend this right to deceased persons or to their nominees in respect of posthumously discovered data. This means that embarrassing medical records, private correspondence, or intimate photographs of deceased persons may remain accessible online indefinitely, capable of being used against surviving family members' dignity and reputation without any legal avenue for removal.

ARTIFICIAL INTELLIGENCE, DIGITAL RESURRECTION, AND THE FUTURE OF POSTHUMOUS PRIVACY

Artificial intelligence has developed over decades through successive breakthroughs in mathematics, computing, and machine learning. Generative AI tools now make it possible to create highly realistic simulations of deceased persons, recreating their voice, appearance, mannerisms, and even conversational patterns from digital traces left during their lifetime. These technologies raise profound questions about identity, dignity, and the ethics of reanimating the dead for commercial, artistic, or personal purposes.

Indian courts have begun to address the protection of living persons' personality rights against AI-generated misuse. In *Amitabh Bachchan v Rajat Negi*, 2022, the Delhi High Court restrained unauthorised use of the actor's voice and image for commercial purposes.¹⁹ In *Anil Kapoor v Simply Life India*, 2023, the Delhi High Court extended protection to AI-generated content, deepfake videos, and digital replicas, holding that personality rights must evolve alongside technology.²⁰ Significantly, the court also acknowledged the interests of family members in preventing the tarnishing exploitation of the actor's persona, a recognition that carries direct relevance to posthumous contexts, where family members may be the primary, and indeed the only, holders of any enforceable interest. In *Arijit Singh v Codible Ventures LLP*, 2024, the Bombay High Court safeguarded the singer's voice and unique artistic style from unauthorised AI cloning, recognising the voice as a constitutive element of personal identity.²¹

These decisions, while significant, share a common limitation: all three concerned living persons who were able to litigate in their own right. Indian courts have not yet ruled on

¹⁹ *Amitabh Bachchan v Rajat Negi & Ors* CS (COMM) 819/2022

²⁰ *Anil Kapoor v Simply Life India & Ors* (2023) SCC OnLine Del 6914

²¹ *Arijit Singh v Codible Ventures LLP & Ors* (2024) SCC OnLine Bom 2445

whether personality rights survive death or whether the deceased's family can restrain the creation of AI-generated avatars, deepfakes, or digital resurrections. The common law tradition and the judicial approach evident in the cases discussed in Part IV suggest that personality rights terminate at death. This leaves a regulatory vacuum in which AI companies may commercially exploit deceased persons' voices, images, and data without legal constraint, absent only the platform's own terms of service.

The threat is not merely theoretical. AI companies are known to use publicly available data, including the digital outputs of deceased persons, to train large language and image generation models. Deceased performers' voices have been replicated for commercial recordings without their estates' consent. Chatbot services have simulated deceased relatives for grieving family members, raising serious questions about informed consent, psychological harm, and the dignity of the dead. In the United States, the case of *Raine v OpenAI*, 2025, while concerning a living minor rather than a deceased person, illustrates the capacity of AI systems to cause irreversible harm when safety guardrails are bypassed, a cautionary parallel for the posthumous context.²²

WAY FORWARD: TOWARDS A COMPREHENSIVE LEGAL FRAMEWORK

The foregoing analysis reveals a consistent pattern: Indian law has not kept pace with the digital transformation of identity, property, and legacy. The DPDPA 2023, the IT Act 2000, and the succession statutes collectively fail to provide a coherent, rights-protective framework for posthumous digital existence. The following reforms are proposed.

Amendment of the DPDPA 2023 to Cover Deceased Persons: Section 14 of the DPDPA 2023 should be expanded to provide that the data protection rights of a deceased Data Principal, including rights of access, correction, erasure, and portability, may be exercised by a designated nominee or, in the absence of nomination, by a legal heir as determined by applicable succession law.²³ A time-limited posthumous protection period modelled on Germany's thirty-year standard should be prescribed, after which personal data may be treated as a public record subject to proportionate access rules.

²² *Mathew Raine et al. v OpenAI et al.* [2025] Case No CGC-25-628528

²³ Digital Personal Data Protection Act 2023, s 14

Recognition of Digital Assets in Succession Law: The Indian Succession Act, 1925, should be amended to include an explicit definition of ‘digital assets’ encompassing social media accounts, email accounts, cloud storage, cryptocurrency wallets, NFTs, Demat accounts, domain names, and digital subscriptions.²⁴ These assets should be classified into transferable assets (those with financial value capable of inheritance) and non-transferable assets (those whose character is purely personal, such as private communications). Default rules should govern intestate digital estates in the absence of a valid will or nomination.

Legal Recognition of Digital Wills and Digital Executors: The IT Act 2000 and the Indian Succession Act 1925 should be amended, or separate legislation enacted to recognise electronic wills as legally valid testamentary documents, subject to authenticated electronic signatures and registration through a National Electronic Will Registry. The position of ‘digital executor’ should be formally recognised in statute, with defined powers to locate digital accounts, manage access credentials, administer financial digital assets, and ensure that sensitive personal information is not improperly disclosed. The Information Technology (Amendment) Bill, 2025, provides a potential legislative vehicle for some of these reforms and should be expanded accordingly.²⁵

Regulation of Posthumous AI Resurrection: India urgently requires specific regulation governing the creation of AI-generated avatars, deepfakes, and digital resurrections of deceased persons. Such regulation should require:

- the explicit prior consent of the deceased, expressed in a will, digital will, or other authenticated instrument;
- in the absence of such consent, the informed consent of the deceased's immediate family;
- prohibition on commercial exploitation of AI-generated likenesses of deceased persons without consent; and
- takedown mechanisms enabling families to demand the removal of unauthorised digital resurrections.

²⁴ Indian Succession Act 1925

²⁵ Information Technology (Amendment) Bill 2025

The Digital India Act, currently under development by the Ministry of Electronics and Information Technology, should incorporate these provisions.

Mandatory Platform Compliance and Data Broker Regulation: Technology platforms operating in India should be required by statute to incorporate India-specific succession clauses in their terms of service, providing a legally binding pathway for legal heirs to access, manage, or close the accounts of deceased persons without requiring court orders in every case. Separately, data brokers who acquire and monetise the data of deceased persons for advertising, AI training, or other commercial purposes should be required to obtain the consent of the deceased's estate or, in the absence of an estate, should be prohibited from commercial use of such data for a prescribed period.

Adoption of a RUFADAA-Inspired Framework: India should draw on the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), adopted across many United States jurisdictions, as a model for comprehensive digital asset succession legislation.²⁶ RUFADAA establishes a clear hierarchy: the deceased's explicit online tool designation takes precedence, followed by instructions in a valid will; followed by a terms-of-service agreement; with fiduciary default access as the final tier. Adapting this framework to the Indian context, with appropriate modifications for India's plural succession laws, would provide a principled, predictable, and rights-protective scheme.

CONCLUSION

This article has examined the status of posthumous privacy in Indian law from multiple perspectives: constitutional doctrine, judicial precedent, comparative frameworks, digital inheritance, and artificial intelligence. The picture that emerges is one of significant and urgent legal inadequacy. Indian courts have consistently held that privacy rights extinguish at death and are not inheritable. The DPDPA 2023, India's most recent and most significant data protection statute, makes no provision for deceased persons. Succession law, designed for a world of tangible property, does not recognise the digital estate. And in the space left by Parliament and the judiciary, technology companies, often foreign, often operating under foreign law, fill the vacuum with their own terms of service.

²⁶ Revised Uniform Fiduciary Access to Digital Assets Act 2020 (US)

The consequences are serious and growing. Deceased persons' data is commercially exploited for advertising and AI training without regulation. Ghost identity theft and posthumous financial fraud affect bereaved families with no effective legal remedy. AI-generated avatars and digital resurrections of deceased persons are created and disseminated without consent. And millions of digital assets are effectively lost to families because the law provides no accessible pathway for inheritance.

The German doctrine of postmortal Persönlichkeitsrechte and the varied legislative experiments of EU member states demonstrate that legal systems can and do protect posthumous dignity without sacrificing freedom of expression or research. India, with its strong constitutional foundation in dignity and its rapidly growing digital population, is well-placed to lead in this area but only if Parliament acts with the urgency the situation demands.

The reforms proposed in Part VIII, amendment of the DPDPA 2023, revision of succession law, recognition of digital wills and executors, regulation of AI resurrection, mandatory platform compliance, and a RUFADAA-inspired framework constitute a coherent legislative agenda. They are neither radical nor unprecedented. What is unprecedented is the continued absence of any legislative response to challenges that already affect hundreds of millions of people. Privacy should not be a right that disappears the moment it is most needed: at the hour of death, and in the years that follow.