



INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 4 | 2026

Art. 35

Extending Privacy Beyond Death: A Constitutional Analysis of Posthumous Data Rights in Digital India

Ayesha Khanum

PhD Research Scholar,

School of Law, Presidency University, Bengaluru

Dr. Mohammed Salim Baithulla Khan

Assistant Professor,

School of Law, Presidency University, Bengaluru

Recommended Citation

Ayesha Khanum and Dr. Mohammed Salim Baithulla Khan, *Extending Privacy Beyond Death: A Constitutional Analysis of Posthumous Data Rights in Digital India*, 5 IJHRLR 498-509 (2026).

Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto & Co. administrator.

For more information,
please contact humanrightlawreview@gmail.com

Extending Privacy Beyond Death: A Constitutional Analysis of Posthumous Data Rights in Digital India

ABSTRACT

The continuous expansion of digital technologies has transformed the way individuals create and leave behind personal data, resulting in digital footprints that continue to exist even after death. These digital remains are both legally and constitutionally challenging and ambiguous. In India, the right to privacy is not only a well-known right that has been established as a fundamental right in the groundbreaking case of Justice K.S. Puttaswamy v. Union of India but also after death, its use is unclear and has been inadequately discussed. This paper aims mainly to discuss the constitutionality and extent of posthumous data rights in India. It examines the question of whether constitutional rights to privacy, dignity and informational autonomy ought to be continued past an individual's lifetime especially in an age whereby digital media represents a major force that manipulates individual information. It identifies a clear regulatory gap in India with respect to posthumous data, raising concerns about access, consent, and the management of digital identities after death. The paper is based on a doctrinal and comparative approach which reviews Indian constitutional principles and changing international practices, such as data protection regimes and digital legacy frameworks. It also takes into account the conflicting interests of the family members, providers of the platform, and the independence of the deceased. The paper states that the concept of posthumous data right should be seen as a continuation of the constitutional right to dignity in Article 21. It proposes the development of a coherent, rights-based legal framework in India that addresses these emerging challenges, ensures platform accountability, and recognizes the importance of preserving dignity in the digital afterlife within an increasingly data-driven Digital India.

KEYWORDS

Digital Remains, Posthumous Data Rights, Right to Privacy, Constitutional Law, Digital Afterlife.

INTRODUCTION

The digital age has transformed not only how individuals live, communicate, and interact, but also how they are remembered.¹ Every online interaction through social media, emails, financial transactions, or cloud storage contributes to the creation of a lasting digital footprint. This data does not fade with death unlike physical possession.² It continues to exist, often forming what is now understood as “digital remains.” These digital traces complicate conventional understandings of identity, ownership, and legal personhood. This raises important questions about how the law should respond to a reality where an individual’s digital presence survives their physical existence.

While technological developments have outpaced legal responses, the constitutional framework offers a useful starting point for addressing these emerging concerns. The importance of dignity, autonomy, and control over personal information is highlighted by the Constitution's protection of privacy as a basic right under Article 21, especially in Justice K.S. Puttaswamy v. Union of India.³ However, the application of these principles has largely been limited to living individuals, making it uncertain what happens to personal information after death.⁴ In a society which is constantly increasing digital interactions, this gap becomes more than theoretical. It has practical implications for families, digital platforms, and the integrity of individual identity.⁵

In order to address these challenges, this study investigates whether constitutional values—in particular, privacy and dignity can be legitimately extended beyond death. It explores the challenges posed by the absence of a clear legal framework in India and analyses how other jurisdictions have begun to respond to similar issues. The paper argues for a rights-based approach that recognises the need to protect digital dignity in a manner consistent with constitutional principles and the evolving realities of Digital India.

¹ Collective Memory as Affirmation: People-Centered Cultural Heritage in a Digital Age, in *HERITAGE AND SOCIAL MEDIA* 13 (Routledge 2012).

² Anne Waagstein, An Exploratory Study of Digital Legacy Among Death-Aware People, 3 *THANATOS* 1 (2014).

³ Madhavi Guruswamy, Justice K.S. Puttaswamy (Ret'd) v. Union of India, 111 Am. J. Int'l L. 994 (2017).

⁴ Jeroen C. Buitelaar, Post-Mortem Privacy and Informational Self-Determination, 19 *Ethics & Info. Tech.* 129 (2017).

⁵ Isabela Granic, Hiroyuki Morita & Hanneke Scholten, Beyond Screen Time: Identity Development in the Digital Age, 31 *Psych. Inquiry* 195 (2020).

CONCEPTUALISING DIGITAL REMAINS IN THE CONTEMPORARY DIGITAL ECOSYSTEM

The concept of “digital remains” refers to the extensive and enduring body of personal data that continues to exist even after an individual’s death.⁶ This includes a wide spectrum of information such as social media profiles, photographs, messages, emails, financial records, biometric identifiers, and even behavioural data generated through algorithmic tracking and digital interactions.⁷ Digital data is intangible, infinitely replicable, and often stored and controlled by private technology platforms rather than by the individual or their family.⁸ Digital remains give rise to a distinctive form of posthumous existence, wherein a person’s digital identity continues to persist, interact, and in certain contexts, evolve within the virtual environment despite their physical absence.

The emergence and expansion of digital remains are closely linked to the growing dependence on digital technologies in everyday life.⁹ In contemporary society, digital platforms have become central to communication, self-expression, social interaction, and economic activity. Social media has transformed personal identity into a curated and continuous digital narrative, where individuals actively construct and project their lives online.¹⁰ Eventually this results in the accumulation of detailed and intimate digital footprints that reflect one’s personality, relationships, preferences, and experiences.¹¹ After death, these digital profiles do not automatically disappear; instead, they may be memorialised, deleted, archived, or remain active, depending on platform policies or the decisions taken by family members or designated contacts. This continued existence of digital identities raises complex questions regarding ownership, control, and the ethical management of personal data after death.

The nature of digital remains is not limited to static data. With

⁶ Edina Harbinja, Tal Morse & Lilian Edwards, *Digital Remains and Post-Mortem Privacy in the UK: What Do Users Want?*, 40 Int’l Rev. L. Computers & Tech. 4 (2026).

⁷ Shubhangi Wadhwa & Shreya Bachwani, *Knowing Me, Knowing You: Behavioural Tracking and the Invisible Algorithms That Shape Our Lives*, J. Info. Tech. Teaching Cases (2025).

⁸ Milica Mijatovic, *Digital Assets and Inheritance Law: Legal Vacuum or New Paradigm*, 4 Sci. Int’l J. 7 (2025).

⁹ Guy Merchant, *Mobile Practices in Everyday Life: Popular Digital Technologies and Schooling Revisited*, 43 Brit. J. Educ. Tech. 770 (2012).

¹⁰ Veronica Barassi & Lorenzo Zamponi, *Social Media Time, Identity Narratives and the Construction of Political Biographies*, 19 Soc. Movement Stud. 592 (2020).

¹¹ Scott A. Golder & Michael W. Macy, *Digital Footprints: Opportunities and Challenges for Online Social Research*, 40 Annu. Rev. Sociol. 129 (2014), <https://www.annualreviews.org/doi/10.1146/annurev-soc-071913-043145>.

advancements in artificial intelligence and data analytics, digital information can be processed and reinterpreted in ways that may simulate or reconstruct aspects of a person's identity.¹² This introduces further complications, as the digital presence of a deceased individual may continue to influence social interactions or even be used in ways that were never intended by them. Such developments challenge traditional legal assumptions that view death as a definitive endpoint for rights and obligations.

Digital remains are not merely technical artefacts or neutral data points; they carry significant emotional, social, and cultural value. For families and loved ones, they often serve as a medium for remembrance, mourning, and maintaining a sense of connection with the deceased. For digital platforms, these remains may represent valuable data assets with economic implications, particularly in data-driven business models. From the perspective of the deceased, this raises critical concerns regarding autonomy, consent, and the preservation of dignity. Conventional ideas of personality, ownership, and legal rights are disrupted when people are unable to control how their personal data is accessed, shared, or used after death.

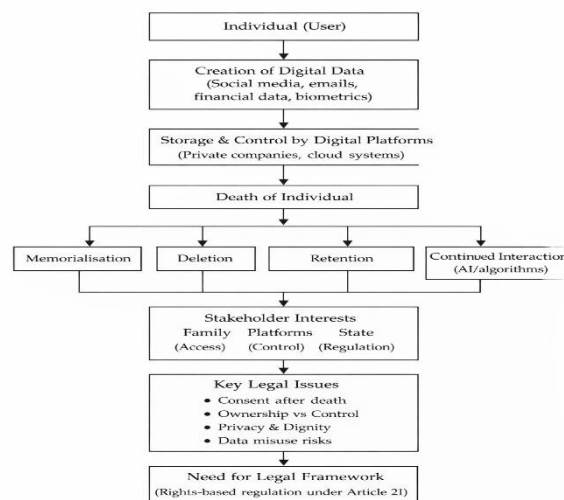


Figure 1: Flowchart Illustrating the Lifecycle and Governance of Digital Remains

As illustrated in *Figure 1*, the lifecycle of digital remains reveals a complex interaction between technological persistence and legal uncertainty.

¹² Kazuhiko Shibuya, *Networked Identity, in Digital Transformation of Identity in the Age of Artificial Intelligence* 147 (Kazuhiko Shibuya ed., 2020), https://doi.org/10.1007/978-981-15-2248-2_10.

The phenomenon of digital remains highlights a fundamental gap in existing legal frameworks, which were not designed to address the persistence and complexity of digital identities. It necessitates a re-examination of legal and constitutional principles to ensure that evolving technological realities are met with appropriate safeguards. Recognising the unique nature of digital remains is thus a crucial first step in developing a coherent approach to posthumous data rights in the digital age.

CONSTITUTIONAL FOUNDATIONS: PRIVACY, DIGNITY AND INFORMATIONAL AUTONOMY UNDER ARTICLE 21

The constitutional framework for analysing posthumous data rights in India is grounded in Article 21 of the Constitution, which guarantees the right to life and personal liberty.¹³ Judicial interpretation has progressively expanded its scope to include rights essential to human dignity.¹⁴ A significant development in this regard was the recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India*, where the Supreme Court affirmed that privacy is intrinsic to dignity, autonomy, and individual development.

Privacy, as recognised in this judgment, is both a negative right against state interference and a positive right enabling individuals to control their personal information. Informational privacy has become particularly significant in the digital age, where personal data is continuously generated and processed.¹⁵ The ability to regulate the use of such data is central to autonomy and self-determination. However, in the context of digital remains, this control ceases after death, creating a legal and constitutional gap.

Indian constitutional law does not explicitly address whether fundamental rights extend beyond death. While rights are generally understood to terminate upon death, the Supreme Court has acknowledged that dignity may persist even after death, as reflected in the recognition of the right to a dignified burial or cremation.¹⁶ This suggests that certain aspects of dignity transcend physical existence.

This raises a critical question: if dignity extends beyond death, can privacy, as its essential component, also be extended posthumously? In

¹³ Sanghmitra Buddhist & Lakshmi Priya Vinjamuri, *Abuse of Power by Law Enforcement Authorities in India with Reference to Human Rights Violation – A Legal Analysis*, 10 *Int'l J. Hum. Rts. & Const. Stud.* 228 (2023).

¹⁴ Paolo G. Carozza, *Human Dignity and Judicial Interpretation of Human Rights: A Reply*, 19 *Eur. J. Int'l L.* 931 (2008).

¹⁵ Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, in *THE ETHICS OF INFORMATION TECHNOLOGIES* 141 (2020).

¹⁶ F. O. Smith, *The Constitution After Death*, 120 *Colum. L. Rev.* 1471 (2020).

the digital context, where personal data remains accessible and vulnerable to misuse, limited protection of informational privacy becomes necessary to preserve dignity.

Extending privacy beyond death is not an expansion of rights, but a logical continuation of the constitutional commitment to dignity under Article 21 in an evolving digital society.¹⁷

LEGAL VACUUM IN INDIA: CHALLENGES OF POSTHUMOUS DATA GOVERNANCE

Despite the growing importance of digital remains, India lacks a comprehensive legal framework to regulate posthumous data rights. Existing laws such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 focus only on living individuals and do not address data after death.¹⁸ This creates a clear regulatory vacuum.

The key challenges include:

- **Access:**

Family members may seek access to digital accounts for emotional or practical reasons, but in the absence of clear law, access is governed by inconsistent platform policies.

- **Consent:**

Consent becomes problematic after death, as individuals can no longer grant or withdraw it. This raises uncertainty regarding whether prior consent continues or whether families or the state should decide.

- **Ownership vs Control:**

While individuals generate data, control rests with platforms through unilateral terms of service, often allowing retention or use of data without accountability.

- **Lack of Digital Estate Planning:**

¹⁷ Ana Dharmo & Iris Dharmo, Right to Privacy and Constitution: An In-Depth Analysis, 11 Interdisc. J. Res. & Dev. 190 (2024).

¹⁸ Medha Kolanu, Rudraksh Lakra & Abhijeet Shrivastava, Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023, 6 Glob. Privacy L. Rev. (2025).

Digital assets are rarely included in wills, leaving families without authority or guidance.

This legal gap not only undermines dignity but also increases risks of data misuse, identity theft, and ethical concerns. A structured legal framework is therefore essential to regulate posthumous data rights in India’s evolving digital landscape.

COMPARATIVE PERSPECTIVES: GLOBAL APPROACHES TO DIGITAL AFTERLIFE AND DATA PROTECTION

The challenges posed by digital remains are not unique to India, and several jurisdictions across the world have begun to address the issue through legislative and policy interventions. A comparative analysis of these approaches provides valuable insights into how posthumous data rights can be conceptualised and regulated within different legal systems.

A comparative overview of different legal approaches to posthumous data governance is provided in Table 1 below.

Jurisdiction	Legal Framework	Posthumous Data Rights	Role of Family / Heirs	Limitations
European Union	General Data Protection Regulation (GDPR)	GDPR primarily applies to living individuals; some member states extend limited rights after death	In certain countries, family members can exercise limited rights over deceased’s data	No uniform rule across EU; posthumous rights vary by country
United States	Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)	Allows management of digital assets after death through fiduciaries	Legal heirs or designated fiduciaries can access digital assets (subject to user consent)	Access depends on prior user consent and platform policies
United Kingdom	Data Protection Act, 2018	Data protection laws generally do not apply after death	Family access governed largely by platform policies and contractual terms	Lack of explicit statutory recognition of posthumous data rights

India	IT Act, 2000 & Digital Personal Data Protection Act, 2023	No explicit recognition of posthumous data rights	No clear legal provision for family access; governed by platform rules	Significant legal vacuum; absence of clear regulatory framework
Platform-Based Regulation (Global)	Company policies (e.g., memorialisation, legacy contacts)	Users may choose settings for their accounts after death	Family may request access or memorialisation depending on platform	Inconsistent policies; lack of legal accountability

Table 1: Comparative Analysis of Posthumous Data Governance

As illustrated above, while jurisdictions such as the United States and certain European countries have taken initial steps towards regulating digital assets after death, India continues to face a significant legal vacuum in this regard.

In the European Union, data protection is governed by a comprehensive framework that emphasises individual autonomy and control over personal data. Although the General Data Protection Regulation (GDPR) primarily applies to living individuals, certain member states have extended limited protections to the deceased. In some jurisdictions, individuals may determine the fate of their data after death, while in others, family members are granted restricted rights of access. This reflects an emerging recognition of posthumous data within the broader framework of privacy and dignity.¹⁹

In the United States, the approach is more fragmented but has evolved through legislation such as the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). This law enables individuals to appoint fiduciaries to manage their digital assets after death, integrating digital data into estate planning while balancing privacy concerns.²⁰

Tech companies have introduced policies such as account memorialisation and legacy contacts. However, these remain inconsistent and governed by private terms rather than uniform legal

¹⁹ Chris Jay Hoofnagle, Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 Information & Communications Technology Law 65 (2019).
²⁰ Luke Lee, *Examining the Legal Status of Digital Assets as Property: A Comparative Analysis of Jurisdictional Approaches* (Apr. 26, 2024).

standards.

These approaches highlight the importance of autonomy, balanced access, and regulatory oversight. For India, a hybrid model combining data protection, estate law, and platform regulation would offer a context-specific and constitutionally aligned solution.

TOWARDS A RIGHTS-BASED FRAMEWORK: EXTENDING DIGNITY BEYOND DEATH IN DIGITAL INDIA

The recognition of posthumous data rights in India necessitates a shift towards a rights-based framework that places dignity at its core. As established under Article 21, dignity is a foundational constitutional value that informs the interpretation of various fundamental rights, including privacy.²¹ If dignity is understood to extend beyond death, then it logically follows that certain aspects of informational privacy should also be protected in the posthumous context.

A rights-based framework for posthumous data governance must begin with the formal recognition of digital remains as a category of personal data deserving legal protection.²² This recognition would provide the conceptual basis for regulating how such data is accessed, managed, and utilised after death. It would also ensure that the treatment of digital remains is guided by constitutional principles rather than purely contractual arrangements.

One of the key components of such a framework is the incorporation of individual autonomy through mechanisms such as digital wills or advance directives.²³ These tools would allow individuals to specify how their digital data should be handled after death, including whether it should be deleted, transferred, or preserved. By enabling individuals to exercise control over their digital legacy, the law can respect their autonomy even in the absence of active consent.

Clear guidelines must be established for granting access to family members and legal heirs. While families may have legitimate interests in accessing digital data, such access must be balanced against the privacy and dignity of the deceased.²⁴ A structured approach that prioritises the expressed wishes of the individual, while allowing limited and regulated

²¹ F. O. Smith, *The Constitution After Death*, 86 *Tenn. L. Rev.* 931 (2019).

²² Henry Pearce, *Our Data? An Examination of the Possible Role of Individual Consent in the Regulation of Posthumous Medical Data Donation (PMDD)*, 45 *Computer L. & Sec. Rev.* 105663 (2022).

²³ S. Gloeckler et al., *Promoting Informed Advance Decision Making in Healthcare*, 22 *BMC Med. Ethics* (2022).

²⁴ Margot E. Kaminski, *The Right to Be Forgotten in the United States: Privacy, Free Speech, and the First Amendment*, 94 *N.C. L. Rev.* 1 (2015).

access in their absence, would help achieve this balance.

Equally important is the need to ensure accountability of digital platforms. Given their central role in storing and managing personal data, platforms must be subject to legal obligations that go beyond their internal policies.²⁵ This includes transparency in data handling practices, compliance with regulatory standards, and safeguards against misuse or unauthorised access. Regulatory oversight is essential to prevent the concentration of unchecked power in private entities.

Finally, legislative intervention is crucial to provide clarity and coherence in this area. A dedicated legal framework addressing posthumous data rights should define key concepts, establish rights and obligations, and provide mechanisms for enforcement. Such a framework must align with the broader objectives of Digital India, ensuring that technological progress does not come at the cost of fundamental rights.

By adopting a rights-based approach that centres on dignity, India can develop a forward-looking legal framework that addresses the complexities of digital remains while upholding constitutional values. This would not only fill the existing legal vacuum but also reinforce the commitment to protecting individual autonomy and dignity in an increasingly digital society.

CONCLUSION

The persistence of personal data beyond death challenges traditional legal frameworks that are premised on the existence of a living individual. As digital technologies increasingly shape identity, communication, and memory, the regulation of “digital remains” has become both urgent and necessary. In the Indian context, although the recognition of the right to privacy under Article 21 represents a significant constitutional development, its application in the posthumous sphere remains uncertain and underdeveloped. This paper has examined the conceptual and constitutional dimensions of posthumous data rights, highlighting the absence of a clear legal framework in India and demonstrating that reliance on platform-based governance is insufficient to address issues of consent, access, and control. Comparative analysis shows that while some jurisdictions have taken initial steps, there is no uniform approach. Central to this discussion is the recognition that dignity, as a foundational constitutional

²⁵ Marvin van Bekkum, Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception?, 48 Computer L. & Sec. Rev. 105770 (2023).

value, does not cease with death. Extending limited aspects of informational privacy beyond life is therefore necessary to preserve autonomy and identity. Accordingly, a rights-based legal framework is essential to regulate posthumous data in India, ensuring that technological advancements align with constitutional values and protect dignity in the digital afterlife.