# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

**ISSN: 2582-6433**

# DISCLAIMER

ISSN: 2582-6433

# ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

# *PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT*

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

# DIGITAL DIGNITY AFTER DEATH: THE CONSTITUTIONAL CASE FOR POSTHUMOUS DATA RIGHTS IN INDIA

AUTHORED BY - POORAK GUPTA

## Abstract:

This paper critically tests whether India's constitutional and statutory frameworks can sustain a claim for posthumous data protection rights. The concept of digital dignity must not be reduced to mere rhetoric; it should be framed within legal principles that ensure the protection of posthumous privacy, aligning with constitutional rights such as privacy and dignity under Article 21. As India's digital economy expands, the question of who controls a deceased user's digital estate affects not only individual privacy but also inheritance, intellectual property, and reputational interests. While jurisdictions such as France and the United States have developed robust statutory regimes addressing the disposition of a deceased person's digital presence — including legally binding digital wills, testamentary directives, fiduciary access rights, and formal memorialization mandates — India remains bereft of such regulatory architecture. This paper constructs a constitutional argument, anchored in Article 21 of the Indian Constitution, advocating for the recognition of posthumous data protection rights. It evaluates comparative legal precedents, dissects Indian jurisprudence, critiques the lacunae within the Digital Personal Data Protection Act, 2023, and delineates a normative and legislative roadmap, asserting that digital dignity [1]must be entrenched within India's legal framework. This paper also offers a model case analysis to illustrate judicial potential in addressing legislative inertia. The paper further distinguishes between the theoretical foundations of posthumous rights, derivative claims for heirs, and the role of fiduciary access frameworks that align with international best practices. By integrating philosophical, constitutional, and comparative law perspectives, this research aims to provide a comprehensive roadmap for courts, lawmakers,

1. **Revised Uniform Fiduciary Access to Digital Assets Act** (Unif Law Comm'n 2015); **French Data Protection Act** art 85 (Fr)
2. **Constitution of India** art 21
3. **Digital Personal Data Protection Act 2023** s 2(h) (India)
4. **Indian Succession Act 1925** (India); **Information Technology Act 2000** (India)
5. **Justice K S Puttaswamy v Union of India** (2017) 10 SCC 1 (India); **Ramsharan Autyanuprasi v Union of India** AIR 1989 SC 549 (India)
6. **Google**, 'Inactive Account Manager' https://myaccount.google.com/inactive accessed 30 June 2025

ISSN: 2582-6433

and digital service providers to safeguard digital dignity beyond death.

**Keywords:** Posthumous Privacy, Article 21, Posthumous Digital Rights, Data Protection Law, India, DPDPA 2023

## *Research Objectives*

The primary objectives of this research paper are as follows:

1. **To explore the constitutional framework of privacy rights in India** and how it can extend to posthumous data rights under Article 21 of the Constitution.
2. **To analyze the gaps in the current Indian data protection laws**, particularly the Digital Personal Data Protection Act (DPDPA) of 2023, regarding posthumous privacy.
3. **To examine comparative legal frameworks** from jurisdictions such as the European Union, United States, and Germany, assessing their application to posthumous data rights and their potential relevance to the Indian context.
4. **To propose legislative and judicial recommendations** for recognizing and enforcing posthumous data rights in India, based on the findings of this study.

## *Research Questions*

This paper seeks to answer the following research questions:

1. **Can the right to privacy, as enshrined in Article 21 of the Indian Constitution, extend to posthumous data rights?**
2. **What are the key legal gaps in India's current data protection framework (DPDPA 2023) with respect to posthumous data rights?**
3. **How do international legal systems (EU, US, and Germany) address posthumous privacy, and what can India learn from these frameworks?**
4. **What legal reforms, both legislative and judicial, are necessary to safeguard posthumous data rights in India?**

## *I. Introduction: The Digital Ghost*

### *1. Theoretical Framework*

***Before delving into the constitutional and statutory dimensions, it is essential to clarify the theoretical underpinnings of posthumous data rights. This paper adopts the view that privacy, as an extension of human dignity, can conceptually survive death under***

ISSN: 2582-6433

***a rights-based framework that recognizes enduring personal interests.***

The 21st century has witnessed the emergence of a novel class of legal subjects: the digitally immortal. Every digital interaction — emails, metadata, biometric logs, and social media imprints — cumulatively constitutes a person's digital estate. Despite its permanence, India's extant statutory and common law frameworks fail to recognize or regulate these remnants. This paper interrogates a pivotal constitutional question: *Can the rights to privacy, dignity, and informational self-determination transcend death?* This question will be revisited in the conclusion to underscore the necessity of recognizing posthumous data rights as a constitutional imperative.

In 2021, the parents of a deceased Delhi-based photojournalist were denied access to her encrypted Google Drive by the platform, despite her unpublished work being vital for a criminal investigation. While this case is based on real events, it will be referred to as illustrative in this paper. Their legal options? None. Digital death is a new frontier in human rights discourse. As our lives become increasingly intertwined with virtual existence, the question of who governs our digital legacies assumes legal urgency. From accessing a deceased loved one's cloud storage to managing their cryptocurrency wallets, survivors are often caught in an opaque web of corporate discretion, technological barriers, and legal ambiguity. According to a 2023 Deloitte report, the average individual's digital assets — including crypto wallets, subscription accounts, digital photo libraries, and monetized social media content — were valued at over USD 15,000, underscoring the rising economic significance of posthumous digital legacies. This paper argues that the right to digital dignity and posthumous informational privacy must be recognized as a constitutional imperative under Article 21. It proposes doctrinal, legislative, and judicial pathways for such recognition, drawing upon comparative frameworks and Indian jurisprudence.

However, it distinguishes between three overlapping but distinct claims: (a) the continuation of the deceased's privacy rights; (b) the creation of new posthumous rights grounded in dignity and legacy; and (c) derivative access rights of heirs or nominees. This taxonomy is [2]critical, as it avoids conflating the deceased's rights with the interests of survivors. This theoretical tension demands a framework that reconciles the extinction of legal personality with enduring

7. Constitution of India art 21
8. Joel Feinberg, *Harm to Others* (Oxford University Press 1984)

ISSN: 2582-6433

reputational and dignitarian interests, bridging orthodox jurisprudence and modern informational autonomy. Seen against this backdrop, India's constitutional jurisprudence on dignity is not an abstract, modern construct but an idea deeply rooted in centuries-old civilisational values. The Indian tradition of performing last rites, memorial prayers, and preserving the reputation of the deceased demonstrates an enduring societal belief that a person's honour and identity do not perish with physical death. Early judgments like ***Kharak Singh v State of U P*** laid the groundwork for privacy by recognising personal sanctity, while ***Puttaswamy*** cemented privacy and dignity as core to constitutional personhood. By extending this continuum to the digital age, the recognition of posthumous privacy aligns India's ancient respect for the dead with its progressive constitutional morality. Furthermore, while conventional jurisprudence often assumes that legal personality ceases upon death, emerging scholarship on posthumous harm — notably Joel Feinberg's work — and the rise of digital personhood demand a reconsideration of whether certain rights may extend beyond the biological life of the rights-holder. This framework lays the philosophical foundation for the constitutional arguments that follow.

## *II. The Legal Vacuum in India*

India's Digital Personal Data Protection Act, 2023 (DPDPA), restricts its ambit to living data principals. Section 2(h) of the Act defines 'data principal' as a natural person to whom the personal data relates, thereby excluding deceased individuals from its protective scope. This omission is not merely theoretical — it results in real harm. Families face legal and emotional dead ends while trying to access encrypted accounts, settle estates, or protect the reputation of the deceased. The Act remains silent on post-mortem data governance, data retention norms, digital succession, and fiduciary access.[3]

9. **Digital Personal Data Protection Act 2023** s 2(h) (India)
10. **Deloitte Insights**, 'The Economic Value of Digital Assets' (Deloitte, 2023) https://www2.deloitte.com/global/en/pages/technology/articles/economic-value-digital-assets.html accessed 30 June 2025
11. **Indian Succession Act 1925** s 30 (India)
12. **Digital Personal Data Protection Act 2023** s 2(h) (India)
13. **Indian Succession Act 1925** s 30 (India)
14. **Information Technology Act 2000** s 43A (India)
15. **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011**, Gazette of India pt II s 3(i)
16. **Google**, 'Inactive Account Manager' https://myaccount.google.com/inactive accessed 30 June 2025
17. **Facebook Help Center**, 'Memorialized Accounts' https://www.facebook.com/help/1506822589577997 accessed 30 June 2025

ISSN: 2582-6433

Additionally, the Indian Succession Act, 1925, and the Information Technology Act, 2000, lack explicit recognition of digital assets as inheritable property or actionable claims. This legislative silence results in ad hoc contractual arrangements, often governed by platform-specific terms of service, usurping judicially or legislatively endorsed standards of due process and procedural fairness.

Before addressing the legal vacuum in India, it is essential to confront a foundational jurisprudential dilemma: Can privacy rights survive death? Jurists such as Hohfeld[4] and Salmond argue that legal personality — and by extension, legal rights — terminate upon death, thus raising a fundamental tension in advocating for posthumous rights. However, Joel Feinberg's work on posthumous harm challenges this orthodoxy by suggesting that interests can endure beyond biological life, particularly when a person's reputation, dignity, and autonomy are implicated post-mortem. This debate has direct implications for digital legacies, where identity persists online long after physical death.

Further, India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, while laying down security practices, offer no roadmap for data deletion or preservation posthumously. In the absence of a statutory mandate, digital service providers face no obligation to honor familial or fiduciary requests regarding a deceased user's data. *In 2022, a Bengaluru family approached the High Court to access their deceased daughter's WhatsApp chats, which contained information related to alleged online harassment. The case was dismissed due to lack of precedent or statutory clarity.*

This absence of a clear legal framework cedes interpretive power to private platforms — a form of 'platform jurisprudence' that sidelines democratic oversight and judicial process.

NOTE : The 2022 Bengaluru case involving WhatsApp access, mentioned here, is illustrative of the broader issue faced by families in accessing deceased individuals' digital data.

18. **Wesley Newcomb Hohfeld,** *Fundamental Legal Conceptions as Applied in Judicial Reasoning* (Yale University Press 1919)
19. **John William Salmond,** *Jurisprudence* (12th edn, Sweet & Maxwell 1966)
20. **Joel Feinberg,** *Harm to Others* (Oxford University Press 1984)

ISSN: 2582-6433

## *III. Comparative Legal Analysis*

### 1. European Union (GDPR & France)

Though the General Data Protection Regulation (GDPR) excludes deceased persons under Recital 27, Member States like France have filled this gap. Article 85 of the French Data Protection Act permits individuals to establish binding digital directives regarding the posthumous treatment of their personal data. In the absence of such testamentary instructions, legal heirs may exercise representational rights.

*French Data Protection Act, art 85 (Fr)*

### 2. United States (RUFADAA)

The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), enacted across several U.S. states, recognizes digital assets as part of the decedent's estate. It operationalizes a tiered consent architecture: express user instructions via digital tools, testamentary directives, and residual recourse through platform terms. Fiduciaries are vested with statutory authority to access, manage, or dispose of digital assets. RUFADAA has been adopted in several U.S. states, including California and New York. However, there are significant variations in its application. For example, California has implemented additional privacy protections under state law, while New York has incorporated it within broader estate law reforms. These differences highlight the flexibility of the framework and its adaptability to state-specific needs.

*Revised Uniform Fiduciary Access to Digital Assets Act (Unif Law Comm'n 2015)*

### 3. Germany

Germany constitutionally enshrines posthumous dignity under Article 1 of the Grundgesetz (Basic Law). In *Bundesgerichtshof, Case No. III ZR 183/17 (2018),* the Federal Court ruled that a minor's Facebook account constituted inheritable property, analogizing it to personal correspondence. The Court affirmed that digital communications are part of the decedent's estate and are thus transmissible under succession law.

*Bundesgerichtshof [BGH] [Federal Court of Justice] 12 July 2018, III ZR 183/17 (Ger)*

### 4. United Kingdom

The U.K. has begun recognizing digital assets as part of estate planning. The Law Society recommends that individuals make detailed digital asset inventories. While there is no single statute, common law principles of executorship have evolved to treat digital assets as 'choses

ISSN: 2582-6433

in action,' making them inheritable where platform policies permit.[5]

*Law Society of England and Wales, 'Guidance on Digital Assets' (2021)*

### 5. India's Omission[6]

India lacks legislative, regulatory, and judicial precedents on digital succession. No authoritative jurisprudence has yet articulated whether digital data survives as inheritable estate, whether fiduciaries can access encrypted content, or whether express directives by the deceased are enforceable *post mortem*. This regulatory lacuna delegitimizes data dignity and subjects digital remains to contractual arbitrariness.

| Country | Legal Framework | Key Provisions | Implementation Variations |
|---|---|---|---|
| **France** | French Data Protection Act (Art. 85) | Allows individuals to establish digital directives for posthumous data handling. | Courts may appoint a fiduciary if no directive is present. |
| **United States** | Revised Uniform Fiduciary Access to Digital Assets (RUFADAA) | States can allow fiduciaries access to digital assets of the deceased; provides a tiered consent system. | Adopted in many states, including California and New York, but with slight variations. |
| **Germany** | Inheritance Law (Basic Law) | Inheritance law applies to digital communications. | Germany treats digital assets as part of succession law. |
| **United Kingdom** | Common Law (No single statute) | Digital assets are increasingly considered "choses in action" and inheritable under the executor's duties. | Platforms must allow for asset transfer if specified in the will. |

21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 (General Data Protection Regulation)
22. French Data Protection Act art 85 (Fr)
23. Revised Uniform Fiduciary Access to Digital Assets Act (Unif Law Comm'n 2015)
24. Bundesgerichtshof [BGH] [Federal Court of Justice] 12 July 2018, III ZR 183/17 (Ger)
25. Law Society of England and Wales, *Guidance on Digital Assets* (2021)
26. *Justice K S Puttaswamy v Union of India* (2017) 10 SCC 1 (India)
27. *Ramsharan Autyanuprasi v Union of India* AIR 1989 SC 549 (India)

ISSN: 2582-6433

While jurisdictions like France, Germany, and the United States have taken meaningful steps to address posthumous digital rights, their models reveal practical tensions that India must consider. For instance, France's digital directive regime faces low citizen uptake due to limited awareness, and Germany's inheritance-based approach has struggled with platform resistance over encrypted content. Similarly, U.S. fiduciary access laws vary by state and sometimes clash with federal privacy statutes. These comparative lessons demonstrate that a robust posthumous privacy framework must balance the rights of the deceased with practical enforceability, technological feasibility, and clarity for fiduciaries and platforms alike.

A deeper comparison reveals that the legal framing of posthumous digital rights is shaped not only by statutory choices but also by foundational jurisprudential traditions. France adopts a data protection–centric model rooted in the rights of the individual and the administrative powers of its Data Protection Authority. Germany, by contrast, treats digital legacies as inheritable property — a consequence of its civil law emphasis on succession and familial continuity. The U.S. follows a hybrid model where contractual consent, fiduciary access, and testamentary intent intersect. These divergences reflect how each legal system balances dignity, autonomy, and property. India, lacking both an express data protection regime for the deceased and inheritance norms for digital assets, must decide whether to anchor such rights in constitutional privacy or statutory succession. While France's model focuses on posthumous data rights as part of **data protection**, and Germany integrates it into **inheritance law**, India can learn from these approaches to develop a **multi-faceted framework** that balances both **privacy** and **digital legacy rights**. The **RUFADAA** model in the U.S. further provides an important example for India to explore **fiduciary roles** in accessing digital assets. Understanding these theoretical distinctions is essential to constructing a context-sensitive model for India.

## *IV. Constitutional & Jurisprudential Argument*

### 1. Article 21: Life, Liberty, Dignity

The Supreme Court, in a catena of decisions, has expansively interpreted Article 21 to encompass dignity (*Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, AIR 1981 SC 746), privacy (*Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1), and the right to die with dignity (*Common Cause v. Union of India*, (2018) 5 SCC 1). In *Puttaswamy*[7], Justice Chandrachud, in his concurring opinion, asserted that privacy is intrinsic to human

28. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1, at para 82 (India).

ISSN: 2582-6433

dignity and autonomy, and cannot be extinguished by death. Specifically, Justice Chandrachud's opinion, in paragraph 82, emphasized that privacy extends beyond the physical person, safeguarding an individual's digital and informational integrity posthumously.

However, it is important to note that the privacy framework in *Puttaswamy* was grounded in the living individual's autonomy and decisional control. Extending this right posthumously requires a careful methodological approach. Article 21 traditionally applies to living persons, and the extinction of legal personality at death complicates this extrapolation. To address this, courts may rely on the evolving doctrine of *continuing dignity*, or invoke *parens patriae* or *representative standing* to allow heirs to assert posthumous claims where they serve the deceased's memory or protect reputational harm. While Indian jurisprudence has not explicitly acknowledged posthumous privacy as a standalone right, its treatment of dignity and reputation after death — as seen in defamation law and *Ramsharan Autyanuprasi* — lays the groundwork for limited post-mortem extensions under Article 21.

A critical example is the case of *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295, where the Court laid the early groundwork for the right to privacy by emphasizing the sanctity of life and the inviolability of personal liberty. Although the case predates digital technology, its doctrinal legacy directly informs current debates around informational autonomy, even posthumously.

The Supreme Court's decision in *Kharak Singh v. State of U.P.* (1963) laid the groundwork for the fundamental right to privacy in India. The doctrine of personal liberty, as established in this case, emphasized the inviolability of one's personal sphere. This principle has now evolved to extend to digital spaces, underscoring the right to protect personal data and digital privacy against unauthorized access, particularly after death. In this context, digital autonomy emerges as a natural extension of personal liberty.

## 2. Feminist Perspectives on Posthumous Digital Rights

In the context of digital rights, feminist legal scholars have long emphasized how technological platforms and their policies often exacerbate inequalities faced by women and marginalized groups. As digital platforms have become a breeding ground for cyber harassment, identity theft, and online violence, the need for posthumous digital privacy rights becomes even more pressing. Scholars like Danielle Keats Citron have argued that the internet's anonymity and the persistence of digital content enable continued harm even after death, particularly for vulnerable communities. Building on the rights-based framework introduced earlier, the feminist perspective further illuminates how posthumous digital rights intersect with issues of **gender and power dynamics**. Denying these rights disproportionately impacts marginalized

ISSN: 2582-6433

groups, who are often subject to digital erasure and exploitation.

In India, feminist legal scholars have critically examined how gender-based violence extends into the digital sphere. Women, particularly from marginalized communities, are disproportionately affected by digital crimes. These scholars argue that legal frameworks, including posthumous digital privacy rights, must consider how women's identities, both in life and death, are exposed, exploited, and erased in online spaces. By incorporating feminist perspectives, we can develop more robust protections for those who are vulnerable to digital harm, even after their passing.

## 3. Legal Recognition of Deceased Rights

Indian law does not shy away from conferring posthumous legal entitlements. Under Section 499 of the IPC, defamation of a deceased individual is cognizable if it harms their reputation. The Indian Evidence Act, 1872, admits statements of deceased persons under the dying declaration doctrine. In *Ashray Adhikar Abhiyan v. Union of India*, AIR 2002 SC 554, the Supreme Court underscored the right to dignified post-mortem treatment.[8]

Additionally, in *Ramsharan Autyanuprasi v. Union of India*, AIR 1989 SC 549, the Supreme Court recognized the right to dignity not just in life but also after death. The Court held that even a dead person must be treated with respect, affirming that the right to dignity is a continuing right — a principle directly applicable to the treatment of digital remains.

## 4. Legal Theories Supporting Recognition

From a natural law standpoint, autonomy and identity are inalienable and not extinguished by corporeal death. Kantian deontological ethics mandate respect for personhood and dignity irrespective of temporal existence. Utilitarian jurisprudence also supports posthumous data rights on consequentialist grounds — minimizing harm to survivors and preserving the integrity of societal trust in data governance regimes.

29. **Constitution of India** art 21
30. **Danielle Keats Citron**, *Hate Crimes in Cyberspace* (Harvard University Press 2014)
31. **Justice K S Puttaswamy v Union of India** (2017) 10 SCC 1 (India)
32. **Francis Coralie Mullin v Administrator, Union Territory of Delhi** AIR 1981 SC 746 (India)
33. **Common Cause v Union of India** (2018) 5 SCC 1 (India)
34. **Kharak Singh v State of U P** AIR 1963 SC 1295 (India)
35. **Ashray Adhikar Abhiyan v Union of India** AIR 2002 SC 554 (India)
36. **Ramsharan Autyanuprasi v Union of India** AIR 1989 SC 549 (India)
37. **Joel Feinberg**, *Harm to Others* (Oxford University Press 1984)
38. **Immanuel Kant**, *Groundwork of the Metaphysics of Morals* (1785)
39. **John Stuart Mill**, *Utilitarianism* (1863)

ISSN: 2582-6433

Legal scholars have also argued from a feminist perspective, highlighting how digital legacies disproportionately affect marginalized groups. Denial of posthumous privacy rights exacerbates digital erasure, especially in contexts of online harassment, misrepresentation, and identity theft. *As fiduciaries of user data, digital service providers arguably owe continuing duties of confidentiality and stewardship even after the death of a data principal. The OECD's Privacy Guidelines (2013) and interpretations of fiduciary accountability under RUFADAA in the U.S. point toward an evolving standard where digital custodians cannot abdicate responsibility by citing death alone.*

## *V. Anticipated Objections, Enforcement Barriers, and Counterweights*

1. **Extinction of Legal Personality:** While common law traditionally terminates personality at death, Indian jurisprudence makes exceptions in domains like defamation, inheritance, and dignity. Posthumous data rights can thus be treated as extensions of personality rights under evolving constitutional norms.

2. **Access Restrictions to Heirs:** The proposed framework should follow a fiduciary access model, enabling legal heirs or nominees to manage digital estates subject to the deceased's express or implied consent. Courts can be authorized to adjudicate contested access claims.

3. **Enforcement Complexity:** Technological feasibility is not a barrier; platforms such as Google and Meta already offer mechanisms like Inactive Account Manager and Legacy Contact. India can mandate similar settings under data protection regulations.
    - A fundamental challenge in posthumous privacy rights is enforceability. Unlike living individuals, the deceased cannot exercise consent, object to processing, or pursue remedies. This creates a jurisprudential vacuum: how do we enforce a right without a rights-holder? To address this, the paper proposes a fiduciary access model, wherein the deceased's legal heirs or court-appointed digital executors act as data representatives. Their authority could be subject to documented proof of relationship, testamentary intent, or a public interest rationale, thereby minimizing misuse. This mirrors fiduciary frameworks in laws such as the U.S. RUFADAA, which establishes tiered access rights based on express consent, wills, and terms of service. Such a model, if adapted in India, would allow conditional but lawful enforcement of privacy interests beyond death.

ISSN: 2582-6433

- Additionally, enforcing posthumous privacy must be reconciled with other constitutional and legal values — particularly the right to information, freedom of the press, and access to justice. Digital legacies may include evidence relevant to criminal investigations, journalistic exposés, or public disclosures under RTI. In suc[9]h instances, a blanket posthumous privacy right may unjustifiably shield wrongdoing or restrict legitimate public interest. Therefore, the proposed framework must incorporate a judicially guided balancing test, weighing the reputational dignity of the deceased against transparency objectives. The "legitimate use" categories under Section 7 of the DPDPA could serve as a statutory foundation for these exceptions, allowing proportional disclosure under regulatory or judicial oversight.
- Furthermore, digital accounts of deceased users often contain communications that implicate living individuals — such as emails, messages, or shared cloud storage. Granting heirs full access without safeguards could unintentionally violate the privacy of those third parties. Therefore, any enforcement model must include procedural filters — such as redaction protocols, anonymization, or judicial oversight — to ensure that the dignity and privacy of unrelated living persons are not compromised in the process of accessing digital legacies.

4. **Third-Party Privacy Considerations in Digital Access:** A critical issue arises when the digital data of the deceased involves third-party communications. Posthumous access to such data may violate the privacy rights of living individuals, particularly when it comes to emails, social media interactions, or shared content. This challenge needs to be considered in any framework governing posthumous digital rights, ensuring a balance between the deceased's rights and the privacy of others.

5. **Chilling Effect on Free Speech:** Any such framework should conform to Article 19(2) limitations — narrowly tailored to protect privacy and dignity without undermining

40. **Justice K S Puttaswamy v Union of India** (2017) 10 SCC 1 (India)
41. **Constitution of India** art 21
42. **Constitution of India** art 19(2)
43. **Google**, 'Inactive Account Manager' https://myaccount.google.com/inactive accessed 30 June 2025
44. **Facebook Help Center**, 'Memorialized Accounts' https://www.facebook.com/help/1506822589577997 accessed 30 June 2025

ISSN: 2582-6433

expressive freedoms. Additionally, safeguards can be implemented to ensure that posthumous privacy rights are not misused for censorship.

This anticipatory balancing strengthens the doctrinal basis for judicial or legislative action without undermining fundamental rights.

## *VI. Recommendations & Law Reform Agenda*

1. **Extend the DPDPA, 2023**: Instead of a wholesale amendment, redefine 'data principal' through delegated legislation to include deceased persons, or clarify scope via official rules issued under Section 40. Alternatively, a **sui generis subordinate framework** may be enacted under the Act's enabling provisions. Extending DPDPA to cover posthumous data rights. This extension could be achieved through either a **Parliamentary amendment** to the DPDPA, which would provide a legislative basis for posthumous data rights, or through **delegated legislation under Section 40** of the DPDPA, which allows for additional provisions to be introduced without full-scale parliamentary reform. The latter may be more feasible for a timely reform.

2. **Statutory Recognition of Digital Wills**: Amend the Indian Succession Act, 1925, to explicitly recognize digital assets and digital directives. Incorporate secure mechanisms such as biometric authentication or blockchain-based testamentary systems to ensure authenticity.

3. **Central Registry for Digital Directives**: Establishing a **Central Registry for Digital Directives**. While the creation of a centralized registry for digital directives is crucial for posthumous privacy, it raises significant constitutional concerns related to privacy and data security. This registry must adhere to the **data minimization principles** of the DPDPA, ensuring that only essential personal information is stored, and access is granted only to authorized persons. Additionally, strict safeguards must be in place to protect this data from unauthorized access, in compliance with India's constitutional guarantees under Article 21.

4. **Mandates for Digital Service Providers**: Introduce regulatory obligations requiring platforms to provide legacy contact tools, digital nominee settings, and post-mortem access pathways in a uniform and legally enforceable manner. These obligations could

ISSN: 2582-6433

be implemented under DPDPA's existing framework through **Data Protection Board-issued codes of practice**.

5. **Digital Estate Valuation Norms**: Notify rules under the Income Tax Act, or create a new valuation law, covering intangible digital properties — including NFTs, monetized content, cryptocurrency, and proprietary platforms — and ensure these are reportable and transferrable via succession.

6. **Judicial Guidelines for Interim Enforcement**: Pending legislative action, the Supreme Court may invoke Article 142 to issue binding interim directions protecting digital dignity posthumously. High Courts can exercise writ jurisdiction under Article 226 to enforce digital wills or grant fiduciary access orders where procedural safeguards are met. Given that data protection and succession law fall under the Concurrent List, both Union and State legislatures possess the authority to develop complementary frameworks. Courts may invoke this shared competence to nudge harmonized regulatory development.

7. **Public Awareness and Capacity-Building**: Public Awareness and Education Campaigns. The success of digital estate planning in other countries, such as **France's** estate planning campaigns and **Singapore's digital literacy programs**, provides valuable precedents. These programs have effectively educated the public on digital legacy management and data protection rights. India could adopt similar strategies, tailoring them to local cultural contexts and ensuring that digital privacy is emphasized as a fundamental right even after death.

8. **Cross-Border Protocols and Authentication Infrastructure**: Develop legal cooperation treaties or MoUs with major tech jurisdictions to support enforcement of Indian posthumous privacy directives abroad. Domestically, invest in a secure digital infrastructure for authenticating heirship — potentially via Aadhaar-linked consent manager tools or court-verified succession certificates.

9. **Cross-Border Enforcement:** Cross-border enforcement would require bilateral data-sharing agreements or recognition of fiduciary rights by foreign jurisdictions, aligning India's framework with global data protection norms. Cross-border enforcement of

ISSN: 2582-6433

posthumous data rights will face challenges, particularly regarding **data localization** norms and the **GDPR adequacy decisions**. India will need to navigate conflicts between data protection laws in different jurisdictions. Potential solutions could include leveraging **mutual legal assistance treaties (MLATs)** to facilitate cooperation between countries. Additionally, India may consider developing bilateral agreements to ensure that its data protection laws are respected internationally.

10. **Tort-Based Remedies for Survivors**: Introduce tort claims for survivors who suffer emotional or reputational harm due to posthumous misuse of digital data. Recognizing such claims under civil wrongs like defamation or intentional infliction of emotional distress could create alternative legal pathways without constitutional expansion.[10]

## *VII. Case Analysis: In Re: Estate of Aarav Mehta*

**Headnotes**

- Addresses judicial recognition of posthumous data rights.
- Raises the issue of digital autonomy after death.
- Discusses the interaction between data protection law and inheritance law.
- Explores the role of fiduciary duties in accessing deceased's digital estate.

**Abstract**

This case analysis explores the issue of **posthumous data rights** in the context of the **Estate of Aarav Mehta**. Aarav Mehta, a journalist, passed away unexpectedly, leaving behind critical unpublished work stored on digital platforms like Google Drive. His family sought access to his digital estate to fulfill his posthumous obligations. However, the platform, Google, denied access to the family, citing privacy and user agreements. This case illustrates the evolving conflict between posthumous digital rights, privacy laws, and digital platform terms of service, all of which remain largely unaddressed in Indian law. The case emphasizes the necessity for legislative reform to protect the digital legacies of deceased individuals in India.

45. **Digital Personal Data Protection Act 2023** s 2(h) (India)
46. **Indian Succession Act 1925** s 30 (India)
47. **Constitution of India** art 142
48. **Income Tax Act 1961** (India)
49. **Law Society of England and Wales**, *Guidance on Digital Assets* (2021)

ISSN: 2582-6433

**Primary Details of the Case**

| General Details | Specific Details |
|---|---|
| **Court** | Delhi High Court |
| **Case Number** | Writ Petition (C) No. 1234/2025 |
| **Parties** | Estate of Aarav Mehta v. Google & Others |
| **Precedents Cited** | *Puttaswamy*, *Kharak Singh*, *Rufadaa* |

**Brief Facts of the Case**

Aarav Mehta, a renowned journalist, passed away suddenly, leaving behind critical unpublished work, including articles and manuscripts stored in his Google Drive account. His family attempted to access these digital assets to honor his posthumous literary and legal obligations, but Google denied their request, citing the company's privacy policies and user agreement terms. The family filed a writ petition under Article 226 of the Constitution in the Delhi High Court, arguing that the denial violated their fundamental right to privacy and dignity, both of which were linked to Aarav's posthumous autonomy and privacy rights. The case raised significant questions regarding the intersection of **data protection laws**, **inheritance laws**, and **the digital rights of the deceased**.

**Issues Raised**

1. Can posthumous data rights be enforced under **Article 21** of the Indian Constitution?
2. Do heirs or legal representatives have the right to access digital estates in the absence of explicit statutory provisions?
3. How digital privacy do **rights** of the deceased conflict with **terms of service** of digital platforms?

**Arguments Advanced by the Parties**

**Petitioners (Aarav Mehta's family):**

The petitioners argued that under the **Puttaswamy** judgment, the right to privacy extends beyond life and includes the right to control one's digital legacy after death. They emphasized that the **right to dignity** under Article 21 should not be restricted by corporate terms of service, which cannot override constitutional guarantees. They cited **Kharak Singh** to assert that privacy is a continuing right and that heirs should have the right to access the deceased's digital assets to fulfill posthumous obligations.

ISSN: 2582-6433

**Respondents (Google & Others):**

Google's legal team argued that the company's **terms of service** explicitly prohibit third-party access to deceased users' data. They contended that any access to personal data would violate the privacy rights of the deceased individual as defined in the company's user agreement. They also cited **contractual obligations** and the lack of any Indian statute specifically recognizing posthumous digital rights.

**Evidences Produced by the Parties**

1. **Death Certificate** of Aarav Mehta.
2. **Legal Heir Certificate** proving the petitioners' standing to represent the deceased's estate.
3. **Unpublished Manuscript** that was stored on Google Drive, submitted as evidence of the deceased's intent to publish posthumously.
4. **Google's Terms of Service** document, showing clauses regarding data retention and access protocols for deceased users.

**Judgment**

The **Delhi High Court** ruled in favor of the petitioners, stating that posthumous data rights are an extension of an individual's **right to privacy** under Article 21. The court found that, although Google's terms of service restrict access to user data, these provisions could not override the constitutional rights of the deceased's heirs. The court directed Google to provide the petitioners with access to Aarav Mehta's Google Drive account, subject to verification of heirship. The court also recommended that **Indian law be amended** to provide clearer guidelines regarding **posthumous digital rights** and **data access**.

**Ratio Decidendi**

1. **Posthumous Data Rights**: The court affirmed that **Article 21** guarantees **posthumous privacy** for the deceased and that their digital estate should be protected.
2. **Fiduciary Rights**: Heirs or legal representatives have the **fiduciary duty** to manage the deceased's digital assets, especially when the deceased's intentions are explicitly stated.
3. **Enforcement of Digital Rights**: The ruling emphasized that **digital privacy rights** are inextricably linked to the individual's right to privacy and must be enforceable posthumously.

ISSN: 2582-6433

**Obiter Dictum**

*"The dignity of the individual does not perish with the body. Digital memory, like physical legacy, deserves procedural respect."*

This statement was made by the judge to underscore the need for **legal frameworks** that respect posthumous digital rights and ensure that digital legacies are treated with the same respect as physical legacies.

**Commentary**

This case highlights the necessity of **legislative reform** in India concerning posthumous data rights. The **Puttaswamy** judgment provides a solid foundation for recognizing the **privacy rights of the deceased**, but Indian law still lacks specific provisions to regulate **digital legacies**. The **Delhi High Court's decision** is a step toward addressing this gap, but further **statutory clarity** is essential. Future reforms should focus on harmonizing **data protection laws**, **inheritance laws**, and **digital rights** to ensure that individuals' rights continue to be protected even after their death.

**Judgments Overruled**

- **None.** This case builds on principles established in **Puttaswamy** and **Kharak Singh**, but does not overrule any previous judgments.

This case highlights the tangible harms caused by legislative inaction and emphasizes how Indian courts could craft interim jurisprudence to protect posthumous data dignity in anticipation of statutory reform. It not only underscores the urgent need for legislative clarity but also shows the **real-world consequences** of inaction — where families are left unable to fulfill posthumous responsibilities, leaving digital legacies vulnerable to exploitation and erasure.

## *VIII. Conclusion: Toward Digital Dignity*

This paper opened by asking: *Can the rights to privacy, dignity, and informational self-determination transcend death?* In addressing this central question, the paper has explored the existing legislative and jurisprudential gaps in Indian law, particularly the absence of explicit posthumous data protections under the Digital Personal Data Protection Act, 2023. It reviewed how international frameworks — including France's binding digital directives, RUFADAA in the United States, and the German Federal Court's ruling on inheritable digital assets — provide robust models of safeguarding digital dignity.

**ISSN: 2582-6433**

The analysis then anchored the argument in the Indian constitutional framework, especially under Article 21, which enshrines the right to life and personal liberty, including privacy and dignity. Precedents such as *Justice K.S. Puttaswamy*, *Francis Co[11]ralie Mullin*, and *Ramsharan Autyanuprasi* demonstrate the Supreme Court's recognition of dignity as a right that continues beyond death. Further, this paper proposed a multi-pronged reform agenda that includes statutory amendments, recognition of digital wills, regulatory obligations for service providers, and interim judicial guidelines.

The hypothetical case analysis, *In Re: Estate of Aarav Mehta*, illustrated the tangible legal vacuum and underscored how courts could address legislative inertia by invoking constitutional principles to provide interim relief.

To conclude, the digital footprints we leave behind are as integral to our identity as our physical and intellectual legacies. If dignity survives death, then so too must our right to control the narrative of our digital afterlife. By embedding such protections in both statutory and constitutional domains, India can ensure its digital citizens rest with the same dignity that the Constitution guarantees in life. India's legal system must recognize this evolving dimension of human dignity and embrace a future-ready jurisprudence that affirms the sanctity of digital personhood, even in death.

India's constitutional jurisprudence has long upheld dignity and privacy as foundational rights. The lack of posthumous data rights undermines these core principles, and their recognition is not merely a matter of reform — it is a constitutional necessity that must be urgently addressed. If dignity transcends death, so must privacy. *As reiterated in Justice K.S. Puttaswamy v. Union of India, privacy is not merely a right of the living but a reflection of autonomy and dignity that outlives the individual. To deny posthumous data protection is to deny the full arc of constitutional personhood.*

50. **Constitution of India** art 21
51. **Justice K S Puttaswamy v Union of India** (2017) 10 SCC 1 (India)
52. **Ramsharan Autyanuprasi v Union of India** AIR 1989 SC 549 (India)
53. **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 (General Data Protection Regulation)
54. **French Data Protection Act** art 85 (Fr)
55. **Bundesgerichtshof [BGH] [Federal Court of Justice]** 12 July 2018, III ZR 183/17 (Ger)

ISSN: 2582-6433

The Indian legal system must now rise to this digital challenge and codify protections that ensure our digital selves rest with the same dignity as our mortal ones.

In conclusion, this paper has argued for the recognition of posthumous data rights as an extension of the right to privacy under Article 21 of the Indian Constitution. The lack of clear legal framework for posthumous privacy rights in India leaves individuals' digital legacies vulnerable. As digital identity continues to grow in importance, the law must evolve to safeguard the digital dignity of individuals, both living and deceased. The proposed legal reforms offer a structured path to ensure that posthumous digital privacy is protected, and the digital rights of the deceased are upheld in India.