SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases

ISSN NO. 2456-9704
Volume 10 Issue 2
www.supremoamicus.org

DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.

ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

-Editorial Team
Supremo Amicus

EXPLOITATION OF DECEASED PERSONS' DATA — THE CASE FOR A UNIFIED LEGAL CATEGORY UNDER INDIAN LAW

By *K. Anu Priyanka*
PhD Scholar *from Tamil Nadu Dr. Ambedkar Law University, Chennai*

ABSTRACT

Nearly ten million Indians die every year. Each death leaves behind a vast digital footprint — Aadhaar-linked medical records, bank accounts, social media profiles, cryptocurrency wallets, and genetic data stored across dozens of platforms. This data does not disappear when a person dies. It continues to exist, continues to carry economic and reputational value, and continues to be exploited. Criminals use deceased persons' Aadhaar numbers to claim welfare benefits. Hospital staff file fraudulent insurance claims using deceased patients' health IDs. Cyber gangs route crores through deceased persons' bank accounts. Courts are called upon by families to remove deceased persons' photographs from social media platforms. These crimes are real, documented, and growing. Yet Indian law treats each of them as a separate, unconnected problem under different statutes — identity fraud here, defamation there, money laundering somewhere else. This paper argues that all of these crimes share one defining characteristic: they target a person who is permanently unable to consent or defend themselves. This paper argues that Indian law must recognise the exploitation of deceased persons' data as a distinct unified legal category, and proposes specific legislative action to address it.

Keywords: Deceased Persons' Data, Digital Identity, Post-Mortem Rights, DPDP Act 2023, Aadhaar, Exploitation, Unified Legal Category, Indian Law

I. INTRODUCTION

Not a single week passes in India today without a documented case of deceased persons' data being exploited. The UIDAI deactivated more than 2.5 crore Aadhaar numbers of deceased individuals between 2024 and 2026 — numbers that were being misused for identity fraud and unauthorised claiming of welfare benefits across more than 3300 government schemes. The ICMR suffered a data breach in 2023 that exposed 81.5 crore Indian medical records, including records of deceased persons whose data sat in hospital databases long after their death. The CAG documented in its Performance Audit Report No. 8 of 2023 that Rs 6.97 crore was paid under Ayushman Bharat for the treatment of 3446 patients who were already dead — their health IDs used to file fraudulent claims. Take the Bank of India case. An officer of the bank defrauded deceased account holders of Rs 16 crore. He was arrested by the Enforcement Directorate. But what specific law addresses the exploitation of a dead person's bank account? There is none. Take the Baitool case. A gang in Madhya Pradesh routed Rs 9.84 crore through a deceased person's account. Same question. Same answer. And then there is RG Kar. The Supreme Court had to directly order every social media platform to remove the name, photographs and videos of a deceased rape and murder victim. Why did the court have to step in? Because no law automatically required the platforms to do this. There was no mechanism and there was no provision.

Look at all of these cases together and one thing becomes obvious. None of them is really a separate problem. They are all the same problem — data belonging to a dead person being exploited because nobody is left to stop it. Indian law has not seen it this way. Each situation is handled under a different statute by a different agency. Police do not know which law applies. Courts have no framework to evaluate the harm. And legislators have not yet connected the dots.

This paper argues that the exploitation of deceased persons' data is not a collection of separate problems.

It is one problem — the targeting of persons who are permanently unable to consent or defend themselves — and Indian law must recognise it as such. The existing Indian legal framework must be amended to establish the exploitation of deceased persons' data as a distinct unified legal category with specific offences, specific penalties, and specific remedies.

II. THE DIGITAL DATA OF DECEASED PERSONS — A GROWING AND UNGOVERNED REALITY

India generates death at scale. Nearly ten million people die in India every year. Each of those deaths leaves behind a digital footprint that no existing Indian law is equipped to govern. A person who dies in India today leaves behind Aadhaar-linked data across every government database they ever interacted with. Their medical records are stored in hospital electronic health record systems. Their bank accounts may hold unsettled balances. Their social media profiles remain active indefinitely. Their cryptocurrency wallets may contain significant economic value that their family cannot access because no legal framework provides for digital asset inheritance. Their genetic data, stored in hospital databases and diagnostic laboratory systems, carries hereditary implications for their living biological descendants.

The problem is not new but it has become urgent. The Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India[1] held that the constitutional right to privacy is a fundamental right of living persons and observed that this right extinguishes upon death. This observation is legally correct. But it has created an unintended consequence — it has been read to mean that the data of deceased persons requires no legal governance at all. From this we can understand that the law has confused the extinction of the individual's right with the extinction of the need to govern the data itself. The data does not disappear when the person dies. The data continues to exist as a material fact, continues to carry economic value, and continues to affect living persons — the family members, the legal heirs, the biological descendants of the deceased.

As Edwards and Harbinja identified as early as 2013,[2] and as Allen and Rothman argued comprehensively in 2024,[3] the governance of deceased persons' data is ultimately not a question of the rights of the dead but a question of the interests of the living. When a deceased person's Aadhaar is misused, it is the living family that suffers the consequences. When a deceased person's medical records are leaked publicly, it is the living family whose reputation is damaged. When a deceased person's bank account is drained through fraud, it is the living legal heirs who lose their inheritance. The exploitation of deceased persons' data is therefore a harm to the living, and the law must treat it accordingly.

III. HOW INDIAN LAW CURRENTLY ADDRESSES EXPLOITATION OF DECEASED PERSONS' DATA — THE FRAGMENTATION PROBLEM

Indian law does recognise three post-mortem rights of deceased persons — the right to a dignified burial, the right to reputation, and the right to estate. The Supreme Court in Ashray Adhikar Abhiyan v. Union of India and Parmanand Katara v. Union of India affirmed that the dignity of deceased persons is protected even after death. Section 356 of the Bharatiya Nyaya Sanhita 2023 protects the reputation of deceased persons against defamation. The Indian Succession Act 1925 and the Hindu Succession Act 1956 govern the distribution of a deceased person's estate to their legal heirs. These are genuine and important protections. But they were designed for a world in which a person's existence — and the harm that could be done to them — was primarily physical.

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

[2] Lois Weithorn Edwards & Edina Harbinja, 'Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased' 26 Cardozo Arts and Entertainment Law Journal 101 (2013).

[3] Anita L. Allen & Jennifer E. Rothman, 'Postmortem Privacy' 123 Michigan Law Review 285 (2024).

3.1 The Bharatiya Nyaya Sanhita 2023

Section 356 of the Bharatiya Nyaya Sanhita 2023[4] protects the reputation of deceased persons against defamation but does not specifically address the misuse of deceased persons' digital identity for fraud or financial exploitation. When a criminal uses a deceased person's Aadhaar photograph, biometric data, or digital identity to impersonate that person for financial gain, Section 356 does not apply because the harm is not to the deceased person's reputation but to their digital identity. When a deceased person's social media account is used to spread misinformation, the existing defamation provision may not cover this since the account was not operated by the deceased. The BNS 2023 treats digital identity misuse, financial fraud, and reputational damage as separate offences under separate provisions — none of which is specifically addressed to the unique vulnerability of deceased persons.

3.2 Succession Law

The Indian Succession Act 1925 and the Hindu Succession Act 1956[5] govern the distribution of a deceased person's estate to their legal heirs. However these statutes were enacted when estate meant physical assets — land, money, jewellery, and tangible goods. They do not contain any specific provision for the succession of Virtual Digital Assets. A cryptocurrency wallet holding lakhs of rupees, a monetised YouTube channel generating monthly income, a collection of Non-Fungible Tokens — none of these are specifically addressed in Indian succession law. The Government of India taxes Virtual Digital Assets at 30 percent under Section 115BBH of the Income Tax Act 1961 thereby treating them as assets of economic value.[6] If the State taxes these assets during a person's lifetime, it must provide a clear inheritance procedure for legal heirs after death. The failure to do so creates a constitutional inconsistency that goes directly to the heart of the exploitation problem — criminals exploit precisely the legal vacuum that the absence of a succession framework creates.

3.3 The Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act 2023[7] is the first data protection legislation in India. Section 14 grants a data principal the right to appoint a nominee to exercise data rights upon death or incapacity. The Digital Personal Data Protection Rules 2025,[8] notified on 13 November 2025, require Data Fiduciaries to publish procedures allowing nominees to act on behalf of deceased persons. These are important steps. But Section 14 and the Rules 2025 leave the vast majority of deceased persons' data entirely unprotected. The nomination right is voluntary — there is no obligation on any person to appoint a nominee. No mechanism exists for persons who die without making any nomination. No enforcement machinery exists to compel platforms to deactivate deceased persons' data after death is reported. The substantive enforcement provisions of the Rules will not become operative until May 2027. From this we can understand that even where legislative action has been taken, the absence of mandatory provisions and automatic implementation mechanisms renders that action practically ineffective.

[4] The Bharatiya Nyaya Sanhita, 2023, Act 45 of 2023 (India), s. 356.
[5] The Indian Succession Act, 1925, Act 39 of 1925 (India); The Hindu Succession Act, 1956, Act 30 of 1956 (India).
[6] The Income Tax Act, 1961, Act 43 of 1961 (India), s. 115BBH (inserted by Finance Act 2022).
[7] The Digital Personal Data Protection Act, 2023, Act 22 of 2023 (India), s. 14.
[8] The Digital Personal Data Protection Rules, 2025, G.S.R. 875(E) (Ministry of Electronics and Information Technology, Government of India, November 13, 2025).

3.4 The Information Technology Act 2000

The Information Technology Act 2000[9] and the Prevention of Money Laundering Act 2002[10] address identity theft, hacking, unauthorised access, and financial fraud as general offences. These provisions are applied to cases of deceased persons' data exploitation only by analogy — there is no specific provision addressing the unique characteristics of this category of crime. The result is inconsistent prosecution, inadequate penalties, and no specific remedies for the families of deceased persons whose data has been exploited.

IV. THE CASE FOR A UNIFIED LEGAL CATEGORY — WHY FRAGMENTATION FAILS

The fragmentation of the existing legal framework is not a minor technical inconvenience. It is a fundamental structural failure that has real consequences. When a criminal uses a deceased person's Aadhaar to claim welfare benefits, the investigating agency must identify which statute applies — is this identity fraud under the IT Act, money laundering under the PMLA, or impersonation under the BNS? When the family of a deceased person wants to compel a social media platform to remove their relative's account, which court has jurisdiction, under which law, and on what specific ground? When a hospital leaks the medical records of deceased patients, which statute imposes liability and what remedy is available to the family?

The answer to each of these questions is unclear because Indian law has not recognised that these situations all belong to the same legal category. They are all instances of the exploitation of deceased persons' data — the targeting of data belonging to a person who is permanently unable to consent or defend themselves. All of these crimes belong to one category. They target data that has no living owner left to defend it.

When a living person is defrauded, they can file a complaint. They can identify what was taken. They can instruct lawyers and pursue the case. When that person is dead, none of this is possible. The data sits there, unprotected, with no one to report its misuse and no one to stop it. The family finds out only after the damage is done. This is not the same as ordinary fraud. It is a category of its own.

The constitutional argument for this unified category is grounded in Article 14 of the Constitution.[11] Persons who die without any legal framework governing their data are treated differently from persons whose data is governed — not because of any rational distinction but purely because of a legislative gap. The families of deceased persons whose data is exploited are denied equal protection of the laws compared to families of living persons whose data exploitation is addressed by specific statutory provisions. Article 21[12] provides further support — the Supreme Court has held that dignity does not end at death.[13] The systematic exploitation of deceased persons' digital identity — using their biometric data to commit fraud, their photographs to create deepfakes, their medical records to file false insurance claims — violates the dignity of the deceased and causes quantifiable harm to their living relatives.

V. THE INJURIES CAUSED BY EXPLOITATION OF DECEASED PERSONS' DATA

The exploitation of deceased persons' data causes at least six distinct categories of injury to living persons

---

[9]The Information Technology Act, 2000, Act 21 of 2000 (India), ss. 43, 66, 66C, 66D.

[10]The Prevention of Money Laundering Act, 2002, Act 15 of 2003 (India), s. 3.

[11]Constitution of India, art. 14.

[12]Constitution of India, art. 21.

[13]Ashray Adhikar Abhiyan v. Union of India, (2002) 2 SCC 27 (India); Parmanand Katara v. Union of India, AIR 1989 SC 2039 (India).

and must be understood in this comprehensive sense for the unified legal category to be properly calibrated.

Financial injury arises when deceased persons' bank accounts, Virtual Digital Assets, or welfare entitlements are misappropriated by third parties leaving legal heirs without their rightful inheritance. The Bank of India fraud of Rs 16 crore and the Baitool cyber fraud of Rs 9.84 crore are documented examples of financial injury caused to the legal heirs of deceased account holders.[14]

Reputational injury arises when deceased persons' digital identities are used to spread misinformation, create deepfakes, or conduct fraudulent activities in the deceased person's name — as in the RG Kar Medical College incident where the Supreme Court was compelled to intervene directly.[15]

Constitutional injury arises when legal heirs are denied inheritance rights over Virtual Digital Assets despite those assets being recognised as taxable property by the State under Section 115BBH of the Income Tax Act 1961.[16] This creates an arbitrary distinction incompatible with Article 14 of the Constitution.

Genetic and hereditary injury is a category Indian law has completely ignored. Think about what happens when a hospital leaks the genetic data of a deceased patient. That data does not belong only to the person who died. A deceased person's child carries 50 percent of that genetic information. So does a sibling. So do parents. None of them consented to have their genetic information stored in that hospital's database. None of them were told it was at risk. But when a breach happens they are affected — permanently. You cannot change your DNA after a leak. This is what makes deceased persons' genetic data different from every other category of personal data and why it needs specific legal protection.

Psychological and emotional injury is real and documented. When a deceased person is digitally impersonated through deepfakes or AI-generated content, the family is forced to watch their relative's face and voice being used to commit crimes or spread lies. There is no law in India today that specifically addresses this harm.

Privacy injury to living relatives happens because the data of a deceased person does not exist in isolation. It is connected to the data of living family members — through shared medical histories, joint accounts, and family relationships. When a deceased person's data is exploited, the private information of their living relatives comes out with it. Those relatives had no say in how the deceased person's data was handled and no warning that it would one day be used against them.

VI. WHAT OTHER COUNTRIES HAVE DONE — AND WHAT INDIA CAN LEARN

France was the first country in the world to give persons the right to leave instructions for their digital data after death. Article 85 of the Law for a Digital Republic 2016[17] allows any person to specify in advance how their personal data should be handled after their death — whether preserved, deleted, or transferred to a specific person. This is a voluntary framework but it establishes legal recognition for post-mortem data governance.

China's Personal Information Protection Law 2021[18] gives the relatives of a deceased person the right to

[14]Enforcement Directorate, Press Release on Bank of India Staff Officer Arrest (Ministry of Finance, Government of India, July 2025).
[15]In Re: RG Kar Medical College and Hospital Rape and Murder Incident, Suo Motu Writ Petition (Criminal) No. 1 of 2024, Supreme Court of India (August 2024).
[16]The Income Tax Act, 1961, Act 43 of 1961 (India), s. 115BBH (inserted by Finance Act 2022).
[17]Loi pour une République numérique [Law for a Digital Republic], No. 2016-1321 (France, October 7, 2016), art. 85.
[18]Personal Information Protection Law of the People's Republic of China, 2021, art. 49.

ISSN 2456-9704 www.supremoamicus.org

exercise data rights over the deceased person's information. China saw the problem and passed a law. India has not done even this much.

In the banking sector, the Reserve Bank of India issued the Settlement of Claims in Respect of Deceased Customers of Banks Directions 2025[19] specifically to address deceased bank customers' accounts. Yes, it only covers banking. Yes, it uses manual processes. But here is what matters — India's own central bank has officially put its name to the statement that this is a governance problem that needs fixing. When the RBI says there is a problem, Parliament cannot pretend it does not exist.

India is not alone in facing this problem. But India is alone in doing nothing about it. France passed a law. China passed a law. Even our own banking regulator has officially said the governance gap needs to be fixed. What India is missing is not awareness of the problem. What India is missing is the political will to treat it as one unified problem and pass one unified law to address it.

VII. RECOMMENDATIONS — THE CASE FOR LEGISLATIVE ACTION

In my opinion the absence of a unified legal framework for deceased persons' data exploitation is not a minor gap that can be filled by judicial interpretation or administrative action. It requires specific legislative intervention. The following amendments are recommended.

The Bharatiya Nyaya Sanhita 2023 should be amended to add a specific provision criminalising the exploitation of deceased persons' digital identity for financial gain, reputational damage, or commercial exploitation. Section 356 currently addresses defamation of deceased persons[20] but does not cover the misuse of digital identity, biometric data, or account credentials of deceased persons for fraud. A new provision should establish a specific offence of digital identity exploitation of a deceased person with enhanced penalties reflecting the permanent inability of the deceased to consent or defend themselves.

The Digital Personal Data Protection Act 2023 should be amended to make the nomination right under Section 14 mandatory for all data principals above the age of eighteen and to establish a default governance framework for persons who die without making any nomination.[21] The amendment should also prescribe specific enforcement obligations for Data Fiduciaries — including mandatory deactivation or memorialisation of deceased persons' accounts within a prescribed period after death is reported to them — with specific penalties for non-compliance.

The Indian Succession Act 1925 should be amended to specifically include Virtual Digital Assets within the definition of property for purposes of testamentary and intestate succession.[22] Platform obligations to cooperate with legal heirs and procedures for transfer of digital assets without private keys should be established through subsidiary legislation.

All of these amendments should specifically use the phrase exploitation of deceased persons' data as a unified legal characterisation — establishing across Indian statute law the recognition that crimes targeting the data of deceased persons constitute a distinct category requiring a coherent and comprehensive legislative response.

VIII. CONCLUSION

India faces a documented and growing problem of deceased persons' data exploitation. The UIDAI has

[19] Reserve Bank of India, Settlement of Claims in Respect of Deceased Customers of Banks Directions, 2025 (RBI/2024-25/145, Reserve Bank of India, 2025).

[20] The Bharatiya Nyaya Sanhita, 2023, Act 45 of 2023 (India), s. 356.

[21] The Digital Personal Data Protection Act, 2023, Act 22 of 2023 (India), s. 14.

[22] The Indian Succession Act, 1925, Act 39 of 1925 (India); The Hindu Succession Act, 1956, Act 30 of 1956 (India).

deactivated 2.5 crore Aadhaar numbers of deceased persons misused for fraud. The CAG has documented crores in fraudulent insurance claims filed using deceased patients' health IDs. Courts are being asked to remove deceased persons' photographs from social media because no automatic legal mechanism exists requiring platforms to do so. Bank accounts of deceased persons are being systematically drained by criminals who face no specific legal provision addressing their conduct.

Indian law currently treats each of these as a separate problem under a different statute. This fragmentation is the problem. These crimes share one defining characteristic — they all target persons who are permanently unable to consent or defend themselves. That characteristic is what makes the exploitation of deceased persons' data a distinct unified legal category, and it is what justifies a specific legislative response.

France has acted. China has acted. India's own banking regulator has officially acknowledged the governance gap. Parliament must now act — not with piecemeal amendments to individual statutes but with a coherent recognition that the exploitation of deceased persons' data is a distinct legal category that requires a comprehensive and unified legislative response. The families of ten million Indians who die every year deserve nothing less.

*****

REFERENCES

I. Statutes

1. The Indian Succession Act, 1925 (Act 39 of 1925)
2. The Hindu Succession Act, 1956 (Act 30 of 1956)
3. The Income Tax Act, 1961 (Act 43 of 1961), s. 115BBH
4. The Registration of Births and Deaths Act, 1969 (Act 18 of 1969)
5. The Information Technology Act, 2000 (Act 21 of 2000)
6. The Prevention of Money Laundering Act, 2002 (Act 15 of 2003)
7. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act 18 of 2016)
8. The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 356
9. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 14
10. Constitution of India, arts. 14 and 21

II. Cases

11. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
12. Shakti Yezdani v. Jayanand Jayant Salgaonkar, (2023) 2 SCC 1
13. Ashray Adhikar Abhiyan v. Union of India, (2002) 2 SCC 27
14. Parmanand Katara v. Union of India, AIR 1989 SC 2039
15. In Re: RG Kar Medical College and Hospital Rape and Murder Incident, Suo Motu Writ Petition (Criminal) No. 1 of 2024, Supreme Court of India

III. Reports and Official Documents

16. Comptroller and Auditor General of India, Performance Audit Report No. 8 of 2023 on Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (CAG, Government of India, 2023)
17. Unique Identification Authority of India, Annual Report 2025-26 (UIDAI, Government of India, 2026)
18. Reserve Bank of India, Settlement of Claims in Respect of Deceased Customers of Banks Directions, 2025 (RBI/2024-25/145)
19. Digital Personal Data Protection Rules, 2025 (G.S.R. 875(E), Ministry of Electronics and Information Technology, November 13, 2025)

IV. Journal Articles

20. Lois Weithorn Edwards & Edina Harbinja, 'Protecting Post-Mortem Privacy: Reconsidering the

Privacy Interests of the Deceased' 26 Cardozo Arts and Entertainment Law Journal 101 (2013)
21. Edina Harbinja, 'Post Mortem Privacy 2.0: Theory, Law and Technology' 31 International Review of Law Computers and Technology 26 (2017)
22. Anita L. Allen & Jennifer E. Rothman, 'Postmortem Privacy' 123 Michigan Law Review 285 (2024)
23. Syed Sarfaraj Hamid, 'Legal Status of a Dead Person: A Critical Analysis in the Light of Jurisprudence' 7 Scholar International Journal of Law Crime and Justice 474 (2024)
24. Harigovind P.C. & Rakesh P.S., 'Posthumous Justice: A Socio-Legal Interpretation of Rights of the Dead' 6 Journal of Law and Legal Reform 41 (2025)

V. Foreign Legislation

25. Loi pour une République numérique [Law for a Digital Republic], No. 2016-1321 (France, October 7, 2016), art. 85
26. Personal Information Protection Law of the People's Republic of China, 2021, art. 49