FROM ASHES TO ALGORITHMS: REIMAGINING THE RIGHT TO DIGITAL DEATH IN INDIA'S DATA PROTECTION AND SUCCESSION LAWS

K. KAVYA [1]*& P. GANESH*[2]

ABSTRACT

A person's practical connection with the world is no longer terminated by death as human existence becomes increasingly integrated into digital surroundings. Digital remnants of the departed, such as social media profiles, cloud-stored content, cryptocurrency holdings, personal data repositories, and algorithmically maintained online presences, are not recognised or controlled in India. This article investigates whether Indian law should acknowledge a legally binding "Right to Digital Death," which is defined as a person's antemortem and postmortem right to control the course of her digital life. It critically assesses the Digital Personal Data Protection Act, 2023 and finds that, due to its person-centric consent architecture and silence on the temporal extension of data rights beyond death, the Act is fundamentally unable to address post-mortem data governance.The article examines the succession legal framework, including Muslim personal law, the Hindu Succession Act of 1956, and the Indian Succession Act of 1925, and it finds a structural gap with regard to digital identities and assets. The article establishes a framework based on constitutional values of privacy, dignity, and autonomy under Article 21 as interpreted in Justice K S Puttaswamy (Retd) v Union of India, drawing on comparative insights from Germany's Federal Court of Justice, the United States' Revised Uniform Fiduciary Access to Digital Assets Act, the European Union's GDPR, France's Digital Republic Act, and United Kingdom approaches A model Digital Legacy and Succession (Amendment) Bill, the introduction of statutory digital wills, and modifications to the DPDP Act are among the specific legislative recommendations made in the article's conclusion, which adds a novel doctrinal contribution to Indian data law study.

Keywords: Digital Death; Post-Mortem Privacy; Digital Legacy; DPDP Act, 2023; Succession Law; Digital Assets; Data Protection; Testamentary Succession.

---

[1] K. Kavya, Law Student LLM, Government Law College, Villupuram
[2] P. Ganesh, Law Student LLM, Government Law College, Villupuram

I. INTRODUCTION

The line separating digital presence from biological existence is now irreversibly blurred. Over the course of a lifetime, a modern person creates a layered and legally complex digital estate that includes social media accounts, email repositories, cloud-stored intellectual property, subscription entitlements, personal data held by data fiduciaries, and, increasingly, cryptocurrency wallets and non-fungible tokens. According to traditional doctrine, death eliminates legal personhood, but this finality is not present in the digital realm. Existing legal categories are seriously challenged by the idea of "digital remains," which is the accumulated informational residue of an individual's online activity. These remnants occupy a normative gap that Indian law has not yet filled; they are neither strictly non-transmissible dignitary interests nor exclusively personal property. Constitutional rights doctrine has historically assumed a living rights-bearer, succession regimes consider tangible and intangible property of established legal character, and data protection frameworks are based on the agreement of a living data principal.

This article investigates whether Indian law should acknowledge a "Right to Digital Death," which is defined as a living person's compound right to specify how her digital existence will be treated after death and the corresponding duty on data fiduciaries, courts, and successors to respect that designation. It's not only an intellectual question. India produces exabytes of personal data every year, with more than 800 million internet users as of 2023. In the absence of a legislative framework, this data is vulnerable to the capricious policies of private platforms, the insufficient procedures of current succession legislation, and the DPDP Act's silence about deceased individuals.

The article is structured as follows. The Right to Digital Death is conceptualised in Part II along with its philosophical foundations. The DPDP Act of 2023 is examined in Part III in relation to deceased people. Part IV looks at the gap in succession law. In Part V, a comparative analysis is conducted. In Part VI, significant court rulings are examined. Foundations of the Constitution are examined in Part VII. A legislative framework is proposed in Part VIII. This finishes Part IX.

II. CONCEPTUALIZING THE RIGHT TO DIGITAL DEATH

As a social and legal phenomena, "digital death" cannot be reduced to a single legal event or moment. Mayer-Schönberger noted that digital information persists forever until purposefully erased, in contrast to biological amnesia. When applied to individuals, this implies that long after biological death, the digital self may endure and continue to be used for profit. Therefore, three overlapping issues must be addressed in the legal order: who controls or owns digital remains; who has the authority to make choices regarding them; and whether the deceased's expressed wishes have any legal significance.[3]

Digital assets can be divided into a number of valuable categories. First, personal data is information maintained by platforms, healthcare providers, or financial organisations that can be used to identify or identify a real individual. The second category is digital property, which includes things like bitcoin, domain names, NFTs, and platform-stored material that the user is contractually or proprietarily entitled to. Third, digital identities, such as email addresses, social media profiles, and online personalities that function as both intimate expression repository and communication tools. Fourth, cloud-based content, which includes images, documents, and artistic creations kept on servers owned by third parties and frequently subject to terms of service that claim to end access following death.[4]

The idea of post-mortem privacy, which refers to the deceased's and her loved ones' right to manage material that might harm their reputation, dignity, or grieving process, was primarily created in Anglo-American and European studies. It uses the concept of informational self-determination, which is linked to the 1983 Volkszuhlungsurteil (Census Decision) of the German Constitutional Court, which established that people have a basic right to decide how their personal information is disclosed and used. Harbinja has made a strong case that this right does not immediately expire following death since the justification for informational control the preservation of autonomy and dignity retains normative force with regard to information created during life.[5]

---

[3] Lilian Edwards and Edina Harbinja, 'Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World' (2013) 32 Cardozo Arts & Entertainment Law Journal 83, 88.

[4] James Norris, Digital Death: Mortality and Beyond in the Online Age (Praeger 2016) 22–35.

[5] Rachael Craufurd Smith and others, 'Digital Inheritance in the UK: Property Law and Technology' [2020] Edinburgh Law Review 1.

In terms of philosophy, it is not new to extend autonomy and dignity after death. Defamation law recognises posthumous reputational interests; courts uphold testamentary wishes long after the testator passes away; and copyright law safeguards writers' moral rights after death. There is no justification for excluding the domain of personal data if legal systems consistently respect the potential property and expression rights of non-living individuals.[6]

III. INDIA'S LEGAL VACUUM: CAN THE DPDP ACT, 2023 PROTECT THE DEAD?

India's largest legal action in data governance to date is the DPDP Act 2023. However, the living data principle defined in section 2(j) as a real person to whom personal data belongs and who is competent to exercise rights under the Act is the foundation of its architecture. [7]The Act gives data principals the ability to access information, fix errors, remove data, and give or revoke consent for processing. The deceased, their legal heirs, or their authorised nominees are not granted any of these rights by the text.

A data principal may designate a person to execute her rights in the case of incapacity or death through the notional nominee procedure provided by Section 14 of the Act.[8] There are three structural reasons why this provision is insufficient. First, it is optional rather than required: data fiduciaries are not required by law to notify users about the nominee function or to assist in its use. Second, the nominee has no independent foundation for controlling data that the data principal had not explicitly addressed; instead, the nominee's rights are wholly derivative, allowing them to exercise just those rights that the data principle could have exercised.

Third and most importantly, given the percentage of India's digital population that has never used the nominee provision, the Act offers no default norms for data governance in the event that no nominee has been nominated. This situation would be demographically widespread. The Act's silence on what happens to personal data when the data principle passes away exacerbates this structural deficiency. Data fiduciaries

[6] Antoinette Rouvroy, 'Privacy, Data Protection, and the Unprecedented Challenges of Human Genome Databases' (2008) 2 Journal of Information, Communication and Ethics in Society 310.

[7] DPDP Act (n 3) s 2(j) ('data principal').

[8] DPDP Act (n 3) s 14 (nominee mechanism). The provision is permissive and does not address general post-mortem data governance.

are not required by the Act to remove, store, transfer, or otherwise handle personal data after death. The Act does not provide a method for the withdrawal of consent by operation of law, nor does it grant a successor the right to request erasure or preservation, even though the consent that permitted processing during life expires upon the principal's death.[9]

It's instructive to compare with the European GDPR. Recital 27 makes it clear that the Regulation does not apply to the personal information of people who have passed away, but it also gives Member States the authority to create national regulations pertaining to such information. [10]In response, a number of European nations, most notably France, Italy, and Estonia, have enacted laws governing post-mortem data. Such subsidiary law is not prohibited by India's DPDP Act, but it is also not positively mandated.[11] The nomination system is somewhat elaborated in the draft Digital Personal Data Protection Rules 2025, but the larger governance gap is not addressed. As of right now, the Data Protection Board, the Act's enforcement architecture, lacks the authority to decide post-mortem data disputes.[12]

IV. THE SUCCESSION LAW GAP: ARE DIGITAL LEGACIES INHERITABLE?

The two main succession laws, the Hindu Succession Act of 1956 and the Indian Succession Act of 1925, were not designed to handle digital estates because they were passed before the internet. Whether digital assets qualify as "property" under these regulations and are therefore transmissible upon death is the main question.[13]Although the Indian Succession Act of 1925 provides a broad definition of property, courts have not definitively addressed whether digital assets, online

---

[9] Personal Data Protection Bill 2019 (India), cl 3(14) defined 'personal data' without temporal extension beyond death; compare GDPR Recital 27.

[10] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, Recital 27 ('GDPR').

[11] Ministry of Electronics and Information Technology, Draft Digital Personal Data Protection Rules 2025 (2025) r 13 (nominee and consent manager provisions).

[12] DPDP Act (n 3) s 25 (Data Protection Board); ss 26–27 (adjudication and penalties).

[13] Indian Succession Act 1925 (n 4) s 59 (testamentary capacity); ss 63–65 (formal requirements for wills).
Hindu Succession Act 1956 (n 4) s 6 (as amended by the Hindu Succession (Amendment) Act 2005, Act 39 of 2005); see also Vineeta Sharma v Rakesh Sharma (2020) 9 SCC 1.

accounts, or personal data are covered. [14]A thing is considered property under classical property law if it can be owned, transferred, and has commercial worth. These requirements are met by cryptocurrency, which is a decentralised, transferrable, and valuable asset. Additionally, domain names are identifiable property. Though it is created by the data principle and regulated on her behalf, personal data kept by a third-party data fiduciary is held and handled by the fiduciary rather than being "owned" by the data principal in the traditional sense.There is no heritable interest in the common law sense because social media accounts are managed by terms of service that usually forbid transfer and end access upon death.[15]

A unique but similarly ambiguous stance is presented by Muslim personal law. In India, Islamic inheritance law is based on a fixed share (faraid) system that applies to certain types of property. Classical fiqh does not acknowledge the concept of "digital property," and Indian courts have not established law regarding the application of faraid principles to online accounts or crypto-assets. Family members of a deceased Muslim person have no legal basis to demand access to or control over digital estates, therefore the silence is not benign.[16]

The Indian Succession Act's formal requirements for valid wills writing, attestation, and probate were created for paper documents, thus while testamentary succession offers a partial solution, it has a clear shortcoming. In India, a "digital will" a document outlining how digital assets are to be disposed of has no clear legal standing. The appointment of a "digital executor" with particular authority to handle digital legacies, access platforms, and overturn terms of service is not governed by any legal framework. Even a properly written testamentary document might not be enforceable against data fiduciaries in the absence of such authorities.[17] The doctrinal result is a structural paradox: Indian succession law in its current form may acknowledge the abstract idea that digital property is heritable, but it offers no way for the heir to realise

[14] Indian Succession Act 1925 (n 4) ss 211–222 (probate and letters of administration); s 2(h) ('property').

[15] Rohan Agarwal, 'Digital Assets and Succession Law in India: Towards a Legislative Framework' (2022) 7 National University of Juridical Sciences Law Review 112, 124.

[16] Mulla, Principles of Mahomedan Law (21st edn, LexisNexis 2018) ss 30–42; Mohd Ahmed Khan v Shah Bano Begum AIR 1985 SC 945.

[17] Usha Tandon and Shruti Midha, 'Digital Assets and Succession: The Indian Lacuna' (2023) 12 Delhi University Law Journal 77, 89.

that inheritance against a data fiduciary acting in accordance with the deceased's data protection obligations.

V. COMPARATIVE PERSPECTIVES: LEARNING FROM FOREIGN JURISDICTIONS

The German Federal Court of Justice's 2018 ruling in III ZR 183/17, also referred to as the Facebook Inheritance Case, is the most important comparable development. The Court ruled that platform terms of service that purport to limit inheritance of account access were invalid and that the contractual relationship between a social media user and a platform is part of the user's heritable estate under German law. The Court reasoned that the right to access private communications is comparable to the right to access physical correspondence: private messages and account data form part of the estate just like letters do. The ruling is noteworthy for its conviction that digital accounts are relational spaces with heritable character rather than just leased services.[18]

Adopted in one form or another in more than forty states, the United States' Revised Uniform Fiduciary Access to Digital Assets Act 2015 creates a tiered priority framework: an online tool (like Google's Inactive Account Manager or Facebook's Legacy Contact) supersedes testamentary instructions; a will, trust, or power of attorney governs in the absence of an online tool; and the platform's terms of service apply in the absence of all instruments. The subtlety of RUFADAA is seen in how it balances the fiduciary's duties, the data principal's privacy concerns, and the legitimate claims of successors a balancing that Indian law has not explored[19].

Although the GDPR's treatment of post-mortem data is purposefully limited at the European level (Recital 27 removes deceased persons from the Regulation's reach), Member State legislation has creatively filled the void. The most sophisticated intervention is France's Digital Republic Act 2016, which explicitly grants people the ability to make decisions about the storage, deletion, and sharing of their personal data

---

[18] Dirk Heckmann and Anne Paschke, 'Post-Mortem Privacy: Inheritance of Personal Data in Germany' (2018) 4(1) European Data Protection Law Review 88, 91.

[19] Revised Uniform Fiduciary Access to Digital Assets Act 2015 (USA) ('RUFADAA'); National Conference of Commissioners on Uniform State Laws, RUFADAA With Prefatory Note and Comments (2015).

while they are still alive and gives a trusted third party or heir the authority to carry out those decisions. [20]Similar laws have been passed by Estonia and Italy, indicating a growing European agreement that post-mortem data should be governed by statute. The Law Commission of the United Kingdom acknowledged the growing necessity of addressing digital assets in testamentary paperwork in its 2017 consultation paper on wills reform, but it did not suggest a comprehensive framework for digital legacies.[21] Indian reformers should be cautioned from expecting that comparative precedents will simply translate, as the lack of a statutory solution in the UK highlights the legislative inertia that characterises this field globally.

The comparative landscape identifies four structural components that any successful regime must include: (i) prospective enshrinement of the data principal's post-mortem wishes during life; (ii) legal recognition of a digital executor with enforceable powers against platforms; (iii) default rules for cases of silence and intestacy; and (iv) balancing post-mortem privacy with the legitimate interests of investigators, heirs, and the public record.

VI. CASE LAW ANALYSIS: PRIVACY, DIGNITY AND THE DIGITAL AFTERLIFE

A. *JUSTICE K S PUTTASWAMY (RETD) V UNION OF INDIA (2017)*

Any examination of Indian privacy rights must start with Puttaswamy. The nine-judge panel overruled M P Sharma v. Satish Chandra and Kharak Singh to the extent that it was contradictory, unanimously ruling that the right to privacy is a basic right under Article 21. According to Chandrachud J's concurrence, one unique and constitutionally protected aspect of privacy is informational self-determination, or the right of persons to govern information about themselves.[22]

Puttaswamy's conceptualisation of privacy as a right based on human dignity and autonomy rather than just physical inviolability makes it relevant to the Right to Digital Death.The assertion that this interest completely stops upon death requires

[20] France, Loi no 2016-1321 du 7 octobre 2016 pour une République numérique [2016] JORF no 0235 ('Digital Republic Act'); Arts 63–64.

[21] Law Commission (UK), Making a Will: Consultation Paper No 231 (2017) paras 6.15–6.22.

[22] Puttaswamy (n 5) [325]–[385] (Chandrachud J, concurring) (informational self-determination and decisional autonomy).

substantial normative justification if the informational self extends beyond any particular datum to the more general matter of identity who one is, how one is known, and what others may learn or do with knowledge about oneself. The doctrinal logic of informational self-determination is intrinsically prospective: an individual exercises this right by making decisions about her information's future use during her lifetime.

B. KHARAK SINGH V STATE OF UTTAR PRADESH (1963)

The first Supreme Court ruling to take the idea of privacy under the Constitution seriously was Kharak Singh.[23] Subba Rao J's dissent claimed that personal liberty under Article 21 included the right to be left alone, despite the majority's conclusion that the Constitution did not establish a general right to privacy. The importance of Kharak Singh for digital death is found in its early recognition of the constitutionally important right to be free from surveillance and unwelcome exposure, rather than in its conclusion, which Puttaswamy replaced. The constitutional tradition established in Kharak Singh should denounce the posthumous surveillance that occurs when a deceased person's data is continuously processed by platforms after death.[24]

C. R RAJAGOPAL V STATE OF TAMIL NADU (1994)

The Supreme Court acknowledged in Rajagopal that the right to privacy encompasses the right to regulate what is published about oneself, or the right to one's own story. The Court ruled that without permission, a person's private information could not be disseminated. When applied to the digital sphere, Rajagopal endorses the idea that an individual's digital narrative, or their cumulative online persona, is a protected interest. The same interest in narrative control that Rajagopal acknowledged is violated by the posthumous monetization of a deceased person's profile data or by advertisers continuing to mine her behavioural data.[25]

D. COMMON CAUSE V UNION OF INDIA (2018)

The right to die with dignity was outlined in Common Cause as part of Article 21. The normative weight of advance directives documents that allow people to express their preferences for medical care during their lifetime despite losing the ability to make

[23] Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295.
[24] Kharak Singh (n 31) [20]; see also Gobind v State of Madhya Pradesh (1975) 2 SCC 148.
[25] Rajagopal (n 32) [26].

decisions for themselves was a major topic of discussion in Chandrachud J's concurrence. The freedom to offer prospective digital instructions has substantial doctrinal backing thanks to Common Cause's constitutional acceptance of prospective autonomy. If the law acknowledges that a person's autonomous decisions made during her lifetime are legally enforceable with regard to how she is treated physically after becoming incapacitated, there is no justification for denying the same recognition to decisions made regarding how her digital identity is handled after death.[26]

E. German Federal Court of Justice — Facebook Inheritance Case (2018)

Despite being ruled under German civil law, the German Court's interpretation offers an important point of comparison. The Court used the well-established rule that personal correspondence, such as letters and diaries, becomes part of the estate and is available to heirs as an analogy. Such correspondence's digital counterparts, such as private messages, private images, and account information, ought to be handled similarly. The Court also dismissed the claim that disclosure to heirs was forbidden by data privacy law, ruling that the GDPR's protections work in the account holder's benefit rather than against her heirs. This reasoning's doctrinal coherence suggests that it be adopted in the Indian context: if the data principal benefits from the constitutional right to privacy, the principal must have the authority to order its exercise for benefit.

VII. The Constitutional Foundations of a Right to Digital Death

Three pillars support the constitutional case for a right to digital death: the right to privacy guaranteed by Article 21; the Puttaswamy-derived notion of informational self-determination; and the developing body of constitutional morality jurisprudence. The Supreme Court has construed the right to life and personal liberty guaranteed by Article 21 to include the right to live in dignity. [27]The postmortem marketing of a person's identity the algorithmic mining of her data after death, the continuation of her profile for advertising revenue violates the dignity interest that Article 21

[26] Common Cause (A Regd Society) v Union of India (2018) 5 SCC 1 ('Common Cause') [199] (Chandrachud J, concurring).

[27] Constitution of India 1950, Art 21; Puttaswamy (n 5) (extending Art 21 to informational privacy).

safeguards if dignity is the constitutional basis of privacy. According to this interpretation, the constitutional right is a right to have one's dignity upheld throughout the foreseeable future, including after death, rather than just a right for the living.

According to Puttaswamy, informational self-determination must be proactive. Typically, exercising one's right involves making decisions, such as approving certain uses, refusing permission from others, and controlling what happens to one's personal data.[28] Making decisions regarding posthumous events is inextricably linked to the right to make future decisions. This is the reasoning behind testamentary freedom, the execution of ante-mortem directives, and the law of trusts; it is not a doctrinal innovation.

According to Navtej Singh Johar, constitutional morality mandates that lawmakers and judges uphold constitutional principles even in situations when public morality or legal tradition have not. [29]The now firmly established constitutional ideals of autonomy, privacy, and dignity have not been applied to post-mortem data governance. This application is required under the constitutional morality doctrine.
However, there are certain fundamental issues that need to be answered. Actio personalis moritur cum persona, the conventional theory that rights terminate upon death, would seem to prohibit post-mortem rights claims. This objection confuses the right's temporal scope (prospective) with its source (the living individual). The reason testamentary wishes are upheld after death is not because the testator still has rights, but rather because the legal system honours people's free will. Digital directions should follow the same reasoning.

The data principal's privacy preferences may clash with the interests of heirs, who may have rightful claims to access a deceased person's communications. This conflict is real but manageable: both interests can be served by a tiered structure where the data principal's directions are given priority but may be overridden in situations of true legal necessity. Criminal investigations, taxes, and historical records are examples of

[28] Alan Westin, Privacy and Freedom (Atheneum 1967) 7.
[29] Navtej Singh Johar v Union of India (2018) 10 SCC 1, [261] (Chandrachud J).

public interest exclusions that must be maintained. A right to digital death shouldn't be used as a defence against justifiable governmental interests. Any legislative framework that incorporates proportionality review can guarantee that the state can only access private digital estates when absolutely essential and under court supervision.

VIII. TOWARDS AN INDIAN FRAMEWORK FOR POST-MORTEM DATA GOVERNANCE

Concrete legislative intervention is supported by the normative analysis presented above. A logical framework based on five statutory procedures is suggested in this section.

A. AMENDMENT TO THE DPDP ACT, 2023

A specific chapter on post-mortem data governance should be added to the DPDP Act. The term of "data principal" should be expanded in Section 2(j) to include the authorised nominee or legal representative of a deceased person for the particular purpose of exercising post-mortem data rights. Section 14A, a new section, should stipulate the following:(i) The rights of erasure, access, and correction survive the death of the data principal and vest in the designated nominee or, in the absence of a nominee, in the legal representative; (ii) Data fiduciaries are required to either execute the data principal's registered directives or notify the nominee of available data for decision-making within ninety days of receiving verified notice of a data principal's death; and (iii) in the absence of a directive or nominee, data fiduciaries must keep the data in restricted access for a predetermined period, after which erasure is the default.[30]

B. RECOGNITION OF DIGITAL WILLS AND DIGITAL EXECUTORS

It is necessary to revise the Indian Succession Act of 1925 to specifically acknowledge "digital testamentary directives" as a legitimate document. [31]The following should be included in a digital will: (a) the types of digital assets and data that are subject to the

[30] Compare Regulation (EU) 2016/679 (General Data Protection Regulation) recital 27 ('This Regulation does not apply to the personal data of deceased persons') while permitting Member States to legislate on post-mortem data processing; see also Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (France), arts 63–65, recognising directives concerning the retention, erasure and communication of personal data after death

[31] Indian Succession Act 1925, ss 2(h), 59 and 63.

directive; (b) the designated digital executor, who will have the power to access accounts, request erasure, transfer assets, archive or distribute specific content; and (c) any particular desires pertaining to platforms, data fiduciaries, or content. Statutory ability to execute post-death directions against data fiduciaries, enforceable before the Data Protection Board or a designated civil court, should be granted to digital executors.

C. MANDATORY PLATFORM MECHANISMS

All data fiduciaries operating in India, such as social media platforms, email service providers, cloud storage companies, and financial platforms, should be required by regulations under the DPDP Act to provide users with a "Inactive or Deceased Account Management Tool" that is comparable to those already implemented by some international platforms. [32]These tools must: (i) enable users to designate a legacy contact or nominee; (ii) indicate whether the account should be transferred, deleted, or memorialised; (iii) allow designated individuals to access selective content; and (iv) be enforceable under Indian law, regardless of any contrary provisions in the platform's terms of service.

D. DIGITAL SUCCESSION TRIBUNAL JURISDICTION

Dedicated adjudicatory infrastructure is needed for disputes pertaining to the digital estates of deceased people, such as disputes between nominees and heirs or between heirs and data fiduciaries. Post-mortem data conflicts should be specifically covered by the Data Protection Board's authority, with provisions for coordination with civil courts that have succession jurisdiction. As an alternative, such conflicts might be resolved more quickly by a specialised Digital Succession Tribunal established within the DPDP Act framework.

E. LAW COMMISSION REFERENCE AND MODEL LEGISLATION

[32] Proposed model drawing on France's Digital Republic Act (n 28) Arts 63–64 and RUFADAA (n 25), adapted for the Indian constitutional context.

The Law Commission of India has not published a report specifically addressing digital succession.[33] The legislation Commission should be formally tasked with conducting a thorough analysis of digital succession legislation and creating a draft Digital Legacy and Succession (Amendment) Bill. A stand-alone framework for digital wills, procedural guidelines for the administration of digital estates, and modifications to the DPDP Act and the Indian Succession Act should all be combined into one bill. In order to prevent the fragmentation that has historically defined Indian data and succession legislation, this consolidation is crucial.[34]

IX. SUGGESTIONS AND RECOMMENDATIONS

A. *STATUTORY RECOGNITION OF THE RIGHT TO DIGITAL DEATH*

The Digital Personal Data Protection Act of 2023 should specifically acknowledge a legally binding "Right to Digital Death" in India. The principles of privacy, autonomy, and dignity would be extended into the digital afterlife by allowing people to decide what happens to their personal information, online personas, and digital footprints after they pass away.

B. *INTRODUCTION OF DIGITAL TESTAMENTARY DIRECTIVES AND DIGITAL EXECUTORS*

It is necessary to update the Indian Succession Act, 1925 to acknowledge digital testamentary directives and wills. It should be possible for people to designate digital executors who have the authority to access, store, transfer, archive, or delete digital assets and accounts in line with the intentions of the deceased.

C. *ESTABLISHMENT OF A NATIONAL DIGITAL LEGACY REGISTRY*

The government may create a safe Digital Legacy Registry where people can enter legally binding post-mortem directives on their personal information and digital assets. A registry like this could make it easier to nominate digital representatives and lessen disagreements between service providers and heirs.

---

33 Law Commission of India, Report No 110: Amendment of Certain Provisions of the Code of Civil Procedure 1908 (1985). No dedicated Law Commission report on digital succession exists as of 2025.

34 European Data Protection Board, Guidelines 3/2019 on Processing of Personal Data Through Video Devices (2020). These illustrate the regulatory layering approach India could adopt.

D. Mandatory Post-Mortem Data Governance Policies for Data Fiduciaries

It should be legally mandatory for online platforms and data fiduciaries to provide clear post-death rules that address memorialization, account access, data transfer, and erasure requests. In digital ecosystems, standardised processes would foster accountability, certainty, and user trust.

E. Balancing Digital Autonomy with Public Interest and Heirs' Rights

The autonomy of the deceased individual and conflicting interests, such as the rightful rights of heirs, platform contractual duties, criminal investigations, and archive or public interest considerations, must be balanced in any system governing digital death. Both excessive state interference and unchecked private control of digital remains would be avoided by a proportionality-based strategy.

X. Conclusion

As this research has shown, India has a substantial and expanding legal gap in the management of digital death. Despite its aspirations to be a comprehensive data protection framework, the DPDP Act 2023 is structurally unable to regulate post-mortem data because its enforcement infrastructure lacks post-mortem jurisdiction, its nominee mechanism is vestigial, and its consent architecture requires a living data principal. Digital executors, digital wills, and the heritable nature of platform-based digital identities cannot be sufficiently addressed by Indian succession law, which was created for a world of physical assets and paperwork. As a result, there is a regulatory gap where private data fiduciaries' unilateral and unaccountable decisions affect the digital remains of hundreds of millions of Indians.

According to the comparative analysis, several countries, including the US, Germany, and France, have acknowledged the shortcomings of their pre-digital legal systems and have passed laws to address them. A Right to Digital Death can flourish in India's constitutional tradition because of its strong privacy jurisprudence, which is based on autonomy and dignity. The idea that the right to govern one's digital identity does not cease with biological death is supported by the logic of Puttaswamy's informational self-determination, Common Cause's acceptance of prospective autonomy, and Rajagopal's acknowledgement of narrative control.

Reform has a normative urgency that goes beyond technical considerations. The inability to control post-mortem data is not a passive omission, but rather a deliberate granting of power to private corporations to exploit what was once a person as algorithms become more sophisticated in curating the identities of the living and the dead. In response, Indian law must acknowledge that passing away shouldn't be seen as an act of digital dispossession. Therefore, the legislative agenda is clear: amend the DPDP Act to grant deceased people data rights; recognise digital executors and wills in succession laws; require post-death account management tools for all data fiduciaries operating in India; and refer the issue of digital succession to the Law Commission for comprehensive reform.