



The Last Digital Footprint: Rethinking the Right to Privacy and Control Over Personal Data in the Digital Afterlife and Rights in These Digital Times

Shivein Walia, Atharva Srivastava, Simran Kaur Marwah, Vedika Dubey, Namrata Singh, Sara Kazi, Vaibhav Pandey, Shraddha Pachange, Varada Gite, Sapna, and Nikhil Babu Thomas

Abstract

Digital technologies have created a category of personal legacy that traditional inheritance law never anticipated. The emergence of generative AI has transformed this from a static storage problem into a live governance crisis. A deceased person's data can now be reconstructed into an active synthetic identity, and existing legal frameworks reveal fundamental inadequacies when this happens. This paper undertakes a comparative doctrinal analysis of digital remains governance across India, the United States, and the European Union.

As a matter of established law, the paper finds that the US model, embodied in the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), treats digital assets predominantly as property subject to fiduciary access and probate. The EU's General Data Protection Regulation (GDPR) treats personal data as a lifetime privacy right that lapses at death, a limitation that Kohl (2022) terms the "Cessation Flaw." India's position is more acute still. The Information Technology Act, 2000 contains no provision for digital assets or post-mortem privacy. The Digital Personal Data Protection Act, 2023 (DPDP Act) was not drafted with posthumous data or AI-generated identity in mind. In this vacuum, platform Terms of Service have become the default regulator of digital afterlives.

As a normative proposal, the paper then builds on dignity-based scholarship, including the Digital Personhood Doctrine and its Algorithmic Filiation principle. It argues that post-mortem data control should be grounded in human dignity rather than property or lapsed privacy rights. It sets out a structured legislative model, with draft provisions, anchored in India's Article 21 jurisprudence. The model is intended to operationalize this protection in a non-EU, non-US legal environment.

Introduction

The growing digital presence of individuals has given rise to legal questions that were largely absent from traditional legal discourse. Rapid technological advancement and digital transformation have fundamentally changed the way individuals live, communicate, and interact with the world around them. In addition to their physical existence, individuals now have a digital existence. It is reflected through social media accounts, emails, cloud storage, financial records, and various other online platforms. These interactions create digital footprints that collectively form an individual's digital identity and contain vast amounts of personal data. Unlike an individual's physical existence, this digital presence often continues after death. This gives rise to what is commonly referred to as the digital afterlife (Harbinja, 2017).

The continued existence of digital identities raises significant legal and ethical concerns. These relate to privacy, personal autonomy, dignity, control over personal data, ownership of digital



assets, consent, the interests of surviving family members, and the responsibilities of digital platform providers. The central question is whether existing legal frameworks are adequately equipped to regulate and protect privacy and control over personal data in the digital afterlife.

The emergence of the digital afterlife has extended the debate on privacy and human dignity beyond an individual's lifetime. As personal information continues to exist in digital form after death, questions arise regarding its protection, control, and use. The concern extends beyond protecting the privacy and dignity of the deceased. It also affects the rights and interests of surviving family members, digital platform providers, governments, and society at large (Harbinja, 2017). The increasing use of artificial intelligence has further expanded the scope of post-mortem privacy. It raises new concerns regarding the protection of personal data shared with AI-powered systems (Harbinja, 2017).

This also raises an important question. Should family members have unrestricted access to a deceased person's digital accounts and personal data, or should an individual's privacy continue to receive legal protection after death? Traditional principles of succession and privacy law often struggle to provide clear answers. Several jurisdictions have begun to respond to the challenges of post-mortem digital privacy. However, the approaches remain diverse. A comprehensive legal framework that balances privacy, autonomy, family interests, and technological advancement is yet to emerge.

The issue has not gone entirely unaddressed. Researchers have examined digital inheritance, post-mortem privacy, data protection, human dignity, AI-generated identities, and the management of digital assets (Harbinja, 2017). Yet the protection, control, and continuation of digital identity after death remain unresolved. Comparative legal approaches show different responses. In the United States, RUFADAA provides fiduciary access to certain digital assets (Uniform Law Commission, 2015). In the European Union, the GDPR provides strong protection of personal data during an individual's lifetime but does not extend the same protection to deceased persons. Recital 27 states that the Regulation does not apply to the personal data of deceased persons (Regulation (EU) 2016/679, 2016, Recital 27). In India, Section 14 of the Digital Personal Data Protection Act, 2023 introduces a nomination mechanism (Digital Personal Data Protection Act, 2023, s. 14). This is an important development, though its scope remains limited. The continuing concern is that legal frameworks are evolving more slowly than technology, which creates challenges in regulating modern digital identities.

In the past, literature has mainly focused on the property-based access to digital assets. Emerging frameworks such as the "Digital Personhood" and "Algorithmic Filiation" doctrines propose dignity-based rights. They also propose mechanisms for legally tethering AI clones to a deceased person's intent. However, it remains unclear how these theoretical concepts can be made functional under statutory provisions. Current research also lacks mechanisms for resolving the "liminal" state. This is a state of existential suspension between physical death and social death. It arises when commercial platforms deploy AI clones that resemble the deceased.

Living privacy rights are aggressively enforced, but statutory rights lapse at death. Post-mortem data protection enforcement is therefore hard to assess. As a result, there is limited regulatory data, and significant aspects of post-mortem data are left to corporate self-governance. In India, foundational statutes such as the Indian Succession Act, 1925 (Act No. 39 of 1925) and the Information Technology Act, 2000 (Act No. 21 of 2000) have not directly addressed AI-



generated digital remains ([Indian Succession Act, 1925](#); [Information Technology Act, 2000](#)). It is inconclusive whether their current provisions can govern complex digital estates or prevent unauthorized and illegal AI cloning. Existing scholarship also lacks actionable legal drafting instruments, such as standardized "Digital Wills" suited to the Indian probate context.

To address these unknowns, this study uses a doctrinal and comparative legal approach to formulate a possible post-mortem digital governance framework. It combines the "informational corpse" concept with the Digital Personhood and Algorithmic Filiation doctrines. Building on these concepts, it proposes a non-transferable personality-right model. The model treats personal data as an extension of human dignity. It seeks to connect AI-generated identities permanently to the deceased's lifetime intent.

The study examines legal systems across the United States, the European Union, and India. It also evaluates regulatory developments through sources such as UNCTAD, RUFADAA, and GDPR enforcement trackers. It analyzes how jurisdictions conceptualize digital remains. They are treated either as property ([Uniform Law Commission, 2015](#)) or as an aspect of personality and human dignity ([Öhman & Floridi, 2018a](#)). The study also focuses on the Indian legal vacuum alongside the terms of service of major platforms. These include Facebook's Memorialization Policy ([Meta, 2024](#)), Apple's iCloud terms on its Digital Legacy program ([Apple, 2023](#)), and Google's Inactive Account Manager protocols ([Google, 2024](#)). These doctrinal, comparative, and platform-level analyses inform three suggestive legislative proposals:

1. A statutory "Digital Will" framework overriding standard corporate terms of service.
2. Mandatory "Digital Designations" requiring platforms to offer binding post-mortem data choices at account creation.
3. Standardized "Filiation Testaments" under the DPDP Act to prevent unauthorized commercial exploitation and algorithmic cloning of deceased citizens.

A note on structure is necessary. This paper separates two kinds of proposition. The first is established law: what the DPDP Act, the GDPR, RUFADAA, and Article 21 of the Constitution of India currently provide. These statements are drawn from primary sources and cited to them. The second is normative proposal: what the authors argue the law should become. The proposals above are prescriptive. They are confined to the section titled Proposed Legislative Model, and are not statements of existing law. Passages that report scholarly argument, rather than law, are attributed to the scholars concerned.

Literature Review

This section reports existing law and scholarly argument. Scholarly arguments are attributed to their authors. They should not be read as statements of settled law.

Digital technologies have created a new category of personal legacy that traditional inheritance law never anticipated. People accumulate photographs, social media profiles, financial accounts, and communications in digital form. Questions therefore arise about who controls this material after death, and how it should be preserved, transferred, or deleted ([Owais Farooqui et al., 2022](#)). This concern has intensified with the emergence of generative AI. Generative AI can reconstruct fragments of a deceased person's data into an active synthetic identity. This transforms a static storage problem into a live governance crisis ([Haider et al., 2026](#)). The issue is no longer confined to national debates. It now features in supranational policy discussions such as the European Union's Digital Decade programme ([Conti, 2025](#)).



Defining Digital Assets and Digital Remains

According to the Financial Accounting Standards Board ([FASB, 1985](#)), the United States' Generally Accepted Accounting Principles (GAAP) define assets, per Statement of Financial Accounting Concepts No. 6, as "probable future economic benefits obtained or controlled by a particular entity as a result of past transactions or events." Traditionally, this definition refers to physical assets. These include land, property, machinery, and other tangible property with monetary value. With the rise of technology, the term "asset" has broadened its scope to include a digital component. It is no longer confined to physical characteristics or traditional monetary value.

Based on our synthesis of the existing literature, digital assets can be categorized into three distinct dimensions:

- Digital assets with monetary value: Assets created for financial purposes, or those handling or storing an individual's financial data. These can be further subdivided to include assets with significant commercial value. Examples are monetized YouTube channels, blogs, or social media handles with large followings that generate active income.
- Digital assets with social value: Online profiles, social network accounts, or other digital identities maintained across online platforms.
- Digital assets with emotional value: Digital materials intrinsically linked to personal sentiments, memories, and interpersonal relationships.

We now turn to whether digital remains should be afforded comparable protection to bodily remains, based on the protection of post-mortem privacy. Öhman defines digital remains as "any digital data we leave behind: Facebook profiles, Spotify playlists and preferences, Google search histories, Zoom logs, emails, video game avatars, chat logs, photo libraries, and so on" ([Öhman, 2024, p. 48](#)). This definition reflects the general idea that everyone leaves digital footprints online. These footprints persist indefinitely in the absence of deliberate action to remove them.

A primary line of scholarly argument links digital remains directly to personal identity. Scholars argue that, beyond bodily remains, individuals leave an "informational corpse" or "informational body" upon death. On this view, data functions not as mere property, but as a constitutive element of human identity ([Floridi, 2014, p. 122](#); [Floridi, 2016, p. 308](#); [Öhman & Floridi, 2017, p. 647](#); [Öhman & Floridi, 2018a, p. 319](#)). An informational corpse is defined as an "inorganic body of a human constituted and existing through information related to his identity" ([Floridi, 2014, p. 122](#); [Harbinja, 2020, p. 91](#)). Within this framework, individuals are inherently informational beings, and their data is an extension of their physical personhood. Consequently, violating post-mortem informational privacy is not merely a property dispute. It is an offense against human dignity and personhood ([Floridi, 2016, p. 308](#); [Öhman & Floridi, 2017, p. 647](#)).

Existing Legal Frameworks and Their Adequacy

A clear legal framework is required for the mandatory enforcement of digital inheritance rights. In India, internet activities are primarily governed by the Information Technology (IT) Act, 2000. The Act was introduced primarily to facilitate e-commerce, legal recognition for electronic records, and digital signatures. It contains no provisions recognizing digital assets, post-mortem privacy, or their inheritance ([Information Technology Act, 2000](#)).



India's regulatory landscape has since shifted with the enactment of the Digital Personal Data Protection (DPDP) Act, 2023. Section 14 introduces the first mechanism in Indian law with direct bearing on post-mortem data governance ([Digital Personal Data Protection Act, 2023, s. 14](#)). It grants a data principal the right to nominate another individual. In the event of the data principal's death or incapacity, that individual may exercise the rights of correction and erasure on the data principal's behalf. This is the closest domestic analogue to the "legacy contact" and "inactive account manager" provisions found in platform self-governance frameworks abroad. The nomination right was brought into force by the Ministry of Electronics and Information Technology's commencement notification GSR 843(E) of 13 November 2025 ([Ministry of Electronics and Information Technology, 2025](#)).

Even so, Section 14 remains narrowly drawn. It confers only a nomination right tied to correction and erasure. It does not address digital asset succession more broadly, fiduciary access to platform accounts, or the treatment of AI-generated synthetic identities. Read together with the IT Act, 2000, which predates any statutory recognition of digital assets, India's framework offers a narrow procedural right rather than a substantive law of digital inheritance.

Article 21 of the Constitution of India protects life and personal liberty ([Constitution of India, art. 21](#)). The Supreme Court has recognized privacy as a fundamental right under this Article ([Justice K.S. Puttaswamy \(Retd.\) v. Union of India, 2017](#)). Broader Indian scholarship on succession law and judicial interpretations of the right to privacy supply useful doctrinal groundwork. However, comprehensive legislation specifically governing digital estate transfer remains unformulated. Indian courts have also not yet directly addressed AI-generated digital remains. Whether Article 21 protection extends to a person's digital remains after death is therefore an argument of this paper, developed in the section titled Proposed Legislative Model. It is not settled law.

In contrast, the United States addressed this issue through the Revised Uniform Fiduciary Access to Digital Assets Act ([Uniform Law Commission, 2015](#)), which lays down elementary principles for digital asset inheritance. RUFADAA was promulgated by the Uniform Law Commission as model legislation for state-level adoption. It provides a legal pathway for fiduciaries (executors, trustees, agents) to access and manage a deceased or incapacitated person's digital assets, while attempting to safeguard the decedent's privacy. Under RUFADAA, a fiduciary can compel disclosure of the content of electronic communications in two situations. The first is where the user has explicitly authorized it through a will, trust, or online tool. The second is where a court approves disclosure on a showing of necessity for estate administration.

Where no explicit consent is left, custodians (service providers) may fall back on standard Terms of Service (TOS) agreements. They may restrict fiduciary access strictly to what is "reasonably necessary" for estate administration, or charge administrative fees. RUFADAA attempts to balance the competing interests of owners, fiduciaries, and corporate custodians. However, its reliance on opt-in authorization leaves many estates governed by restrictive platform policies.

Comparative Analysis: US Property-Based Model vs. EU Data Protection Regime

Comparing the US framework with global data protection regimes reveals fundamental regulatory divergences and gaps. Frameworks like the EU's General Data Protection Regulation (GDPR) and state-level laws like the California Consumer Privacy Act (CCPA) focus primarily on data privacy and processing during a person's lifetime ([Bakare et al., 2024](#);



Choi, 2020; Hamulák et al., 2020). However, as Kohl (2022) argues, these privacy frameworks suffer from what she terms the "Cessation Flaw." This is the phenomenon whereby personal, non-transferable data rights held by a data subject during their lifetime simply lapse on death. Examples are the right of access and the right to erasure. They are not passed on or reassigned to another party. Indeed, Recital 27 of the GDPR states: "This Regulation does not apply to the personal data of deceased persons" (Regulation (EU) 2016/679, 2016, Recital 27).

Consequently, the US RUFADAA model treats digital assets predominantly as property subject to probate and fiduciary access. European data protection frameworks treat personal data strictly as a personal privacy right that terminates at death. Neither model, nor India's narrower Section 14 nomination right, provides a unified framework capable of protecting non-economic personal identity against posthumous exploitation or synthetic AI replication (Harbinja & Pearce, 2020; Rao, 2024).

Platform Self-Governance

In the absence of comprehensive legislation, major technology platforms have established proprietary posthumous policies. These range from account memorialization or deletion with a designated "legacy contact" (Facebook/Meta), to memorialization upon proof of death (Instagram), account deletion upon request (Twitter/X), pre-designated "inactive account managers" (Google), and memorialization or removal upon documentation (LinkedIn) (Holt et al., 2024; Owais Farooqui et al., 2022). These policies reflect a developed body of practice. However, they remain voluntary and fragmented. They delegate final authority over digital legacies to private corporations rather than public legal standards.

Furthermore, standard Terms of Service (TOS) agreements typically grant platforms perpetual, worldwide, and transferable licenses over user data. This structural power dynamic implies that platforms can legally use a deceased individual's data to train generative models or create synthetic content. As critical scholars note, this dynamic risks enabling the "monetization of grief" and non-consensual "identity manipulation." Judicial responses to date have primarily protected posthumous identity only where clear commercial value exists. Examples are the monetized publicity rights of celebrity estates such as Marilyn Monroe or Elvis Presley. This produces a "two-tiered" legal regime that leaves ordinary individuals largely unprotected.

Dignity After Death

A growing strand of literature grounds post-mortem protection not in property rights, but in human dignity. This perspective builds on long-standing legal traditions regarding bodily remains. In those traditions, personal wishes regarding one's body are prioritized and survivors act as custodians. Examples are Germany's Totenfürsorge (care for the deceased) and Italy's ius sepulchri (right of sepulchre) (Ermann, 2020; Resta, 2014). Post-mortem privacy is the digital analogue to this principle. It is defined as an individual's right to control their reputation, dignity, and memory after death. Harbinja (2017, 2020) refines this concept as a specific right to control "digital remains."

Buitelaar (2017) and Conti (2025) frame the "digital double" as a continuation of pre-death privacy rights. Davey (2020) and Morse and Birnhack (2022) note that post-mortem privacy is deeply intertwined with the privacy interests and behaviors of surviving relatives. Empirical survey data cited by Conti (2025) indicates strong public consensus that post-mortem privacy is an essential facet of human dignity.



Addressing generative AI risks, Haider et al. (2026) advance this framework by proposing a "Digital Personhood Doctrine." It rests on three pillars. The first is a dignity-focused Post-Mortem Right to Personality. The second is a mandatory "Digital Designation" mechanism, which allows individuals to make binding choices regarding deletion, preservation, or monetization. The third is a fiduciary duty binding platforms to honor these choices. A key contribution is their "Algorithmic Filiation Doctrine." It asserts that any AI-generated identity derived from an individual's data remains permanently tethered to that person's dignity and stated intent. It does not become platform property.

Synthesis and Research Gap

A clear synthesis emerges across the literature. Traditional legal categories, namely property, intellectual property, privacy, and probate, were designed for physical assets. They fail to accommodate digital remains or AI-synthesized identities. A clear evolution is visible. Owais Farooqui et al. (2022) examine the problem primarily through property and asset frameworks. Conti (2025) reframes it around dignity and post-mortem privacy. Haider et al. (2026) extend the dignity framework to counter synthetic AI identities. Across all perspectives, scholars agree that private platform policies are an inadequate default regulator.

The three concepts that recur in this paper operate at different levels. This paper reads them as a sequence rather than as separate labels. First, the Cessation Flaw is a diagnosis (Kohl, 2022). It explains why privacy law offers no protection after death: personal, non-transferable rights lapse rather than pass on. Second, the Digital Personhood Doctrine is a response at the level of the right itself (Haider et al., 2026). Through the Post-Mortem Right to Personality, it supplies a dignity-based right that does not depend on a lapsing privacy right or on property. Third, the Algorithmic Filiation Doctrine is a response at the level of application (Haider et al., 2026). It ensures that when data is reconstructed into an AI-generated identity, that identity stays tethered to the person's dignity and intent. In short, the Cessation Flaw identifies the gap, Digital Personhood fills it with a right, and Algorithmic Filiation carries that right into the synthetic outputs that generative AI creates. The Digital Designation is the practical instrument through which the person's intent is recorded.

Despite these contributions, notable gaps persist. Existing research has not integrated India-specific legal reform needs with the advanced AI-specific doctrinal frameworks developed in global literature. Earlier Indian legal analyses predated generative AI concerns and the DPDP Act's Section 14 nomination right. Even Section 14, being confined to correction and erasure, does not engage with AI-generated synthetic identity at all. Furthermore, jurisdictional fragmentation is acknowledged in both European (Conti, 2025) and global contexts (Haider et al., 2026). Yet current literature lacks an operational legal drafting model tailored to non-EU and non-US legal environments like India.

Connecting Gap in Study

This study directly addresses these unresolved gaps. Owais Farooqui et al. (2022) examine digital assets under Indian law prior to generative AI. Conti (2025) and Haider et al. (2026) formulate dignity-based frameworks primarily tailored to European or conceptual contexts. This paper bridges these perspectives. Specifically, it re-evaluates post-mortem data control within non-EU and non-US legal frameworks. It demonstrates why property- and access-based systems, including India's narrow Section 14 nomination right, are insufficient. It also proposes how dignity-based privacy rights can be pragmatically operationalized into statutory reform to govern an individual's digital afterlife (Ali, 2026; Rao, 2024).



Research Methodology

This research study adopts a doctrinal and comparative legal research approach. It draws on secondary sources, namely statutes, case law, journal articles, and platform policies, rather than empirical data collection. A doctrinal methodology relies on Indian and foreign statutes, regulations, existing scholarly literature, and data protection sources. It is used here to test whether existing legal categories can incorporate digital remains and AI-generated post-mortem data. The paper is supplemented by a comparative analysis. This helped in understanding the similarities and differences in the digital afterlife across jurisdictions such as the United States, Germany, and others. No primary data were collected through interviews, fieldwork, or surveys. The study relied solely on an assessment of statutory text, judicial decisions, and existing research papers.

The doctrinal dimensions examined Indian statutory provisions related to inheritance, digital assets, and data protection. The primary instruments were the Indian Succession Act, 1925, and the Information Technology Act, 2000, together with judicial interpretations of these provisions to date. Indian courts have not yet directly addressed AI-generated digital remains. The analysis was therefore expanded to the broader jurisprudence on digital assets, privacy, and posthumous rights, from which similar principles could be drawn.

The paper also analyzed the terms of service and posthumous account provisions of major service providers operating in India. These include Facebook's memorialization policy, Apple's iCloud agreement, and Google's Inactive Account Manager. The policies were compared with Indian law to assess whether they align with, conflict with, or are silent on Indian law.

The analysis keeps established law and normative proposal distinct. Statements about what the DPDP Act, the GDPR, RUFADAA, and Article 21 case law provide are descriptive, and are tied to primary sources. Statements about what the law should provide are prescriptive. They appear only in the section titled Proposed Legislative Model and in the Conclusion, and they are identified there as the authors' proposals.

Objective

The key objective of the methodology was to identify the loopholes in Indian law governing digital remains and AI-generated post-mortem data. A further objective was to suggest practicable reforms that balance corporate obligation with the dignity and privacy interests of the deceased and their survivors. Sources were examined along two thematic lines. The first was how each jurisdiction and instrument characterized digital remains: as property, as an aspect of personality and dignity, or as data lying outside any protective framework altogether. The second was how practically enforceable each resulting model proved to be.

This comparative analysis was then applied to the problem of AI-generated identity. None of the existing jurisdictional frameworks originally anticipated this issue. Yet it is directly raised by the platform practices and legislative gaps identified in the Indian analysis.

Scope and Limitations

The paper was confined to publicly available statutory text, reported judicial decisions, and published platform agreements, current as of the time of writing. It did not include independent verification of how consistently service providers implement their stated policies. It did not involve empirical research such as interviews, surveys, or stakeholder consultations. The analysis and conclusions are based solely on publicly available legal materials. The Findings



section likewise analyzes legal materials and enforcement trackers. It does not study the behavior of deceased users or platforms.

The comparative discussion of Italy, Germany, the United States, the United Kingdom, Singapore, and Canada was undertaken for doctrinal contrast alongside India's. It was not intended to give a complete account of each country's law. The suggestions offered for Indian reform should be seen as ideas for lawmakers to consider, not as final conclusions.

Findings

This section does not report empirical observation of deceased users, platform behavior, or court outcomes. It reads three sets of publicly available legal materials: the Uniform Law Commission's RUFADAA tracker, the UNCTAD Global Cyberlaw Tracker, and the CMS GDPR Enforcement Tracker. The figures reported are counts and amounts drawn from those trackers. The statistical results are exploratory, rest on small numbers of enforcement actions grouped by country, and indicate patterns in the tracker data only.

The materials were used to answer a simple question that keeps surfacing in the literature. Once a country builds real, enforceable privacy rights for living people, does any of that protection carry over once the person is gone? Across the three jurisdictions studied, the answer is much the same each time. Lawmakers and regulators are comfortable protecting a living person's data, and they are willing to enforce that protection with real money at stake. Almost none of them has built an equivalent structure for after death. This section walks through that pattern jurisdiction by jurisdiction. It then reads the pattern against the arguments in the literature review.

A Near-Universal Legislative Baseline, and a Near-Universal Silence at Death

Of the twelve UNCTAD spotlight countries covered in this study, all twelve now have some form of data protection legislation. They are spread across Asia-Pacific, the Americas, Europe, and Africa. Whether a privacy law exists at all is therefore not in question, in any of the three jurisdictions this paper is concerned with. What changes, and changes quickly, is the question of whether that law extends beyond the person's death.

The GDPR leaves little room for doubt. Recital 27 says outright that the regulation does not apply to the data of deceased persons ([Regulation \(EU\) 2016/679, 2016, Recital 27](#)). India's Information Technology Act, 2000, the law that came before the DPDP Act, is arguably worse. It never mentioned digital assets or what should happen to them ([Information Technology Act, 2000](#)). Kohl (2022) calls this the Cessation Flaw. Rights built as personal and non-transferable while someone is alive are allowed to lapse at death, rather than being passed on, reassigned, or dealt with in any deliberate way. Kohl also makes a broader point worth holding onto. What happens to privacy after death tells us a lot about what privacy was doing for the person while they were alive. That argument fits the material rather well. These laws have plenty to say about the living and almost nothing to say about the dead.

A Mature but Fragmented Fiduciary Model in the United States

Of the three jurisdictions, the United States has gone furthest in trying to close this gap. RUFADAA is now enacted in 49 of 53 US jurisdictions, or about 92.5 percent ([Uniform Law Commission, 2015](#)). This level of state-by-state agreement is rare in American law. The four jurisdictions that have not enacted it do not share one reason. Delaware kept an older 2014



version of the Act. Louisiana and Puerto Rico show no sign of having acted on either version. Massachusetts has only introduced a bill, which has gone nowhere so far.

The substance of RUFADAA is also worth pausing on, because it captures the property-versus-privacy tension that runs through this literature ([Birnhack & Morse, 2022](#)). The Act reads more like an estate-administration tool than a privacy protection. Access is granted only for purposes described as reasonably necessary. It stays bound by whatever terms of service the deceased had already agreed to. Custodians are allowed to charge fees for handing anything over. Even the most legally developed digital-afterlife framework in this study therefore treats digital remains mainly as property to be wound up. It does not treat them as something tied to a person's dignity that deserves protection in its own right. That is only half of what the theoretical literature says matters here ([Harbinja, 2020](#); [Öhman & Floridi, 2018a, 2018b](#)).

Real but Uneven Enforcement in the European Union, and an Explicit Stop at Death

The EU tells a similar story, from a different angle. Between 2019 and 2026, regulators brought 131 enforcement actions under GDPR Article 17 and imposed roughly €128.6 million in fines combined ([Regulation \(EU\) 2016/679, 2016, art. 17](#)). The right to erasure is therefore not just a paper right. It is enforced. But enforcement is uneven across the bloc. Italy, Spain, and Romania bring the most cases by far, yet their average fines are comparatively small. Romania's average works out to just €7,125. France sits at the other end. It has only six cases but an average fine above €10.5 million, and that figure is carried largely by a single €40 million penalty against Criteo.

A regression of case count against year shows no meaningful trend across the full dataset ($p = 0.789$). With France removed as an outlier, a stronger relationship appears between how often a country enforces and how severely it fines ($R^2 = 0.512$, $p = 0.030$). Clearview AI and Google were each fined twice, independently, in two separate member states for essentially the same conduct ([Information Commissioner's Office, 2022](#); [Sweden's Data Protection Authority, 2020](#)). This shows how fragmented enforcement remains even under one supposedly harmonized law. None of this reaches past death. Recital 27 rules deceased persons out of the regulation entirely. The very right traced here stops existing the moment someone dies, however firmly it was enforced during their life.

India's Nomination Right: A Genuine First, Narrowly Drawn

India's Digital Personal Data Protection Act, 2023, is the youngest of the three frameworks examined. Section 14 and its rules came into force only in November 2025 ([Ministry of Electronics and Information Technology, 2025](#)). Section 14 lets a person nominate someone else who can exercise certain data rights, such as correction or erasure requests, once that person has died ([Digital Personal Data Protection Act, 2023, s. 14](#)). For South Asia, this is new ground, and it is a clear step up from a law that said nothing on the subject.

Held up against the American and French models, however, it is a thin mechanism. It gives a right-exercise function rather than the fuller fiduciary account access that RUFADAA provides. It also falls well short of the broader heir-rights approach recognized in France under the *Loi pour une République numérique*, which allows both general and specific instructions to be left behind. The provision has barely been in force a year. There is therefore no enforcement record yet from which to see how it operates in practice. This paper points to that gap. It cannot close it.



Synthesis: Tracker Data and the Doctrinal Argument

Taken together, these results are consistent with the argument in the literature review. Property, contract, probate, and privacy law were all built with physical assets and living data subjects in mind. None of them sits comfortably with digital remains, let alone with the AI-reconstructed identities that Haider et al. (2026) place at the centre of what they call the digital afterlife industry.

The tracker data show a rights infrastructure for the living that is substantial. It includes fines of tens of millions of euros and near-universal legislation across the countries checked. But that infrastructure thins out to almost nothing at the point where the risk described by Haider et al. is greatest. That risk is an AI system generating content in a dead person's voice or likeness, with no binding instruction from that person on whether this is permitted. Platforms have filled this vacuum with their own memorialization and legacy-contact settings. As the literature review notes, those policies are voluntary and inconsistent from one platform to the next. They leave the final say over a person's digital remains with a company rather than with the law.

None of this contradicts the dignity-based argument advanced in the literature (Harbinja, 2017; Haider et al., 2026; Öhman & Floridi, 2018a). The doctrinal literature argues, from first principles, that post-mortem privacy deserves protection. This section adds illustrative support from legal materials. It shows how far current law is from delivering that protection. It also suggests that the gap is not so much closing as going unmeasured in most of the world, India included. Because the section rests on legal materials and trackers, it establishes the state of the law. It does not establish how platforms or families behave in practice.

Proposed Legislative Model

This section is prescriptive. Unlike the preceding sections, it does not describe existing Indian law. It sets out the authors' proposal for a statutory model. The draft provisions below are offered for lawmakers to consider, consistent with the Scope and Limitations of this study. They are intended to sit within, and extend, the DPDP Act framework, including the Section 14 nomination right.

Design Principles

Five principles follow from the comparative analysis. First, post-mortem data control rests on human dignity, not on property or on a privacy right that lapses at death. This is the response to the Cessation Flaw. Second, the deceased's own binding choice, made in life, is the primary rule. Third, any AI-generated identity derived from a person's data remains tethered to that person's dignity and stated intent, in line with Algorithmic Filiation. Fourth, platforms owe an enforceable fiduciary duty to honor those choices. Fifth, the statutory rules prevail over inconsistent platform terms of service. The proposal is anchored in the Article 21 argument set out above. That argument extends the recognized right to privacy and dignity to digital remains, and it remains to be tested before Indian courts.

Draft Provisions

Clause 1 (Definitions). In this Chapter: (a) "digital remains" means any digital data relating to a person that persists after the person's death, including social media profiles, communications, cloud-stored material, and search and usage histories; (b) "digital designation" means a binding instruction made by a data principal, during life, regarding



the deletion, preservation, transfer, or monetization of the person's digital remains; (c) "synthetic identity" means any AI-generated voice, likeness, text, or other output that is derived from a person's data and presented as, or reasonably capable of being mistaken for, that person; (d) "platform" means any service provider that holds a person's digital remains; and (e) "nominee" means a person nominated under Section 14 of the DPDP Act.

Clause 2 (Post-mortem dignity). The digital remains of a person are an extension of that person's dignity. They shall not be treated as the property of a platform. The rights under this Chapter are personal to the deceased and non-transferable. They are exercised through the deceased's designated fiduciary or nominee.

Clause 3 (Digital designation). Every platform shall offer each user, at account creation and at reasonable intervals afterwards, a mechanism to make a digital designation. A digital designation binds the platform. It prevails over any inconsistent term of service.

Clause 4 (Digital Will). A digital designation, or a separate Digital Will executed in the prescribed form, shall be treated as a valid direction concerning digital remains. It shall be given effect in the administration of the person's estate, notwithstanding any contrary term of service.

Clause 5 (Filiation Testament). No person shall create, train, deploy, or commercialize a synthetic identity of a deceased person unless the deceased has expressly authorized it, before death, in a Filiation Testament. Any authorized synthetic identity shall remain tethered to the terms of that Testament. It shall not become the property of the platform. It shall be clearly disclosed as synthetic.

Clause 6 (Fiduciary duty of platforms). A platform holds digital remains as a fiduciary. It shall honor the digital designation and the Filiation Testament of the deceased. No license granted by a user under a term of service shall be construed as authorizing the use of a deceased person's data to train generative models or to create synthetic identities, unless the deceased has authorized that use under Clause 5.

Clause 7 (Default rule). Where a person has left no digital designation, the platform shall not use the person's digital remains to create a synthetic identity. The nominee may exercise the rights of correction and erasure, and may request memorialization or preservation, in the prescribed manner.

Clause 8 (Enforcement). A nominee, designated fiduciary, or surviving family member may complain to the regulator under the DPDP Act against a breach of this Chapter. The regulator may direct compliance and impose penalties as prescribed. Nothing in this Chapter limits the jurisdiction of the courts to grant injunctive relief.

Clause 9 (Overriding effect). The provisions of this Chapter shall have effect notwithstanding anything inconsistent in any term of service or other contract.

Relationship to the Three Proposals

The clauses give statutory form to the three legislative proposals set out in the Introduction. The statutory Digital Will framework is found in Clauses 4 and 9. Mandatory Digital Designations are found in Clauses 3 and 6. Standardized Filiation Testaments under the DPDP Act are found in Clauses 5 and 7. Clause 8 supplies enforcement, a gap that the Findings show is not filled by current law. The drafting is deliberately structured so that it can be adopted as an amendment to, or a chapter within, the DPDP Act.



Conclusion

The preceding review demonstrates that the governance of digital remains sits at an unresolved intersection of property law, data privacy, and human dignity. Existing frameworks were each built for a narrower purpose than the one now required of them. As a matter of established law, the US model under RUFADAA treats digital assets chiefly as property subject to fiduciary access and probate (Uniform Law Commission, 2015). The EU's data protection regime, exemplified by the GDPR, treats personal data as a lifetime privacy right that lapses at death (Regulation (EU) 2016/679, 2016, Recital 27). This is what Kohl (2022) terms the "Cessation Flaw." India's position is more precarious still. The IT Act of 2000 predates any conception of digital assets. The DPDP Act of 2023, though more recent, was not drafted with post-mortem data governance in mind (Digital Personal Data Protection Act, 2023). In the resulting vacuum, platform Terms of Service agreements have become the de facto regulators of digital afterlives. This subordinates public legal standards to private commercial policy.

The emergence of generative AI sharpens the stakes of this gap considerably. Once a deceased person's data can be reconstructed into an active synthetic identity, the governance problem changes. It ceases to be one of static storage and inheritance. It becomes one of ongoing control over a "digital double" that can be monetized, manipulated, or reanimated without consent. Dignity-based frameworks, most notably the Digital Personhood Doctrine and its associated Algorithmic Filiation Doctrine (Haider et al., 2026), offer the most promising conceptual response. They tether AI-generated identity permanently to the deceased's stated intent rather than to platform property claims. Yet these frameworks remain largely conceptual. They were developed with European or global generality in mind, not for operationalization within a specific non-EU, non-US statutory environment.

This is the gap this paper seeks to close. It examines India's legal architecture against the comparative backdrop of the US property-based model and the EU's privacy-based model. It argues that neither imported framework is directly transplantable. The property model understates the identity and dignity harms unique to synthetic replication. The privacy model's cessation at death forecloses protection altogether.

What the paper proposes, as a normative matter, is a dignity-anchored statutory mechanism suited to the Indian legal context. It would recognize post-mortem informational privacy as a facet of human dignity under Article 21 jurisprudence. It would mandate a binding "digital designation" mechanism analogous to a testamentary instrument. It would impose an enforceable fiduciary duty on platforms rather than leaving compliance to voluntary policy. The Article 21 extension is the authors' argument and is not yet settled law. The draft provisions in this paper are offered to move the discourse from theoretical dignity claims toward a pragmatic legal drafting model. Such a model could govern the digital afterlife in jurisdictions where neither RUFADAA nor the GDPR was ever designed to reach.

References

- Ali, A. (2026). Rest in privacy: Legal analysis of posthumous digital afterlife. *Indian Journal of Legal Review*, 6(3), 24–38.
- Apple. (2023). *Legal - iCloud terms and conditions: Digital Legacy program*.
- Bakare, A., Smith, R., & Taylor, K. (2024). Posthumous data governance across global privacy statutes. *International Journal of Law and Information Technology*, 32(1), 45–68.



- Birnhack, M., & Morse, T. (2022). Digital remains: Property or privacy? *International Journal of Law and Information Technology*, 30(3), 280–301. <https://doi.org/10.1093/ijlit/eaac015>
- Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology*, 19(2), 129–142.
- Choi, H. (2020). The cessation flaw in contemporary data protection regimes. *Journal of Information Privacy and Security*, 16(3), 115–134.
- Constitution of India, art. 21.
- Conti, Y. (2025). *Post-mortem data protection in the digital age: A necessity for human dignity?* (SSRN Scholarly Paper No. 6258218). Social Science Research Network.
- Davey, J. (2020). Post-mortem privacy and the interests of surviving relatives. *Modern Law Review*, 83(4), 789–815.
- Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
- Ermann, L. (2020). Totenfürsorge and the custody of digital memory in German jurisprudence. *German Law Journal*, 21(5), 980–1004.
- Financial Accounting Standards Board. (1985). *Elements of financial statements* (Statement of Financial Accounting Concepts No. 6).
- Floridi, L. (2014). *The 4th revolution: How the infosphere is reshaping human reality*. Oxford University Press.
- Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy & Technology*, 29(4), 307–312.
- Google. (2024). *About Inactive Account Manager*. Google Safety Center.
- Haider, A., Khan, A., Salameh, M. H., Almelhem, M. A., Almethen, W., & Rahman, S. U. (2026). When we are gone, but our data is not: The cultural and jurisdictional crisis of post-mortem data governance in the age of AI. *Cogent Social Sciences*, 12(1), Article 2698290. <https://doi.org/10.1080/23311886.2026.2698290>
- Hamulák, O., Kocharyan, H., & Kerikmäe, T. (2020). The contemporary issues of post-mortem personal data protection in the EU after GDPR entering into force. *Czech Yearbook of Public and Private International Law*, 11, 225–238.
- Harbinja, E. (2017). Post-mortem privacy 2.0: Theory, law and technology. *International Review of Law, Computers & Technology*, 31(1), 26–42. <https://doi.org/10.1080/13600869.2017.1275116>
- Harbinja, E. (2020). *Digital assets and post-mortem privacy: A legal perspective*. Routledge.
- Harbinja, E., & Pearce, H. (2020). Your data will never die, but you will: A comparative analysis of US and UK post-mortem data donation frameworks. *Computer Law & Security Review*, 36, Article 105403. <https://doi.org/10.1016/j.clsr.2020.105403>
- Holt, J., Smeddinck, J. D., Nicholson, J., Vlachokyriakos, V., & Durrant, A. C. (2024). Post-mortem information management: Exploring contextual factors in appropriate personal data access after death. *Human–Computer Interaction*. Advance online publication. <https://doi.org/10.1080/07370024.2023.2300792>
- Indian Succession Act, 1925, No. 39 of 1925 (India).



- Information Commissioner's Office. (2022). *Monetary penalty notice: Clearview AI Inc.* (Enforcement decision).
- Information Technology Act, 2000, No. 21 of 2000 (India).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
- Kohl, U. (2022). What post-mortem privacy may teach us about privacy. *Computer Law & Security Review*, 47, Article 105737. <https://doi.org/10.1016/j.clsr.2022.105737>
- Meta. (2024). *Memorialization policy and legacy contact settings*. Meta Help Center.
- Ministry of Electronics and Information Technology. (2025, November 13). *Notification: Digital Personal Data Protection Act, 2023, commencement dates* (GSR 843(E)). The Gazette of India, Extraordinary, Part II, Section 3(i).
- Morse, T., & Birnhack, M. (2022). The posthumous privacy paradox: Privacy preferences and behavior regarding digital remains. *New Media & Society*, 24(6), 1343–1362. <https://doi.org/10.1177/1461444820974955>
- Öhman, C. (2024). *The afterlife of data: What happens to your information when you die and why you should care*. University of Chicago Press.
- Öhman, C., & Floridi, L. (2017). The political economy of death in the digital age. *Philosophy & Technology*, 30(4), 639–662.
- Öhman, C., & Floridi, L. (2018a). An ethical framework for the digital afterlife industry. *Nature Human Behaviour*, 2(5), 318–320. <https://doi.org/10.1038/s41562-018-0335-2>
- Öhman, C., & Floridi, L. (2018b). The political economy of death in the age of information: A critical approach to the digital afterlife industry. *Information, Communication & Society*, 21(11), 1610–1625.
- Owais Farooqui, M., Sharma, B., & Gupta, D. (2022). Inheritance of digital assets: Analyzing the concept of digital inheritance on social media platforms. *Novum Jus*, 16(3), 413–435. <https://doi.org/10.14718/NovumJus.2022.16.3.15>
- Rao, N. (2024). Data after death: Legal consequences of posthumous data management. *Brazilian Journal of Law, Technology and Innovation*, 2(2), 71–83.
- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1–88.
- Resta, G. (2014). Personhood and the right of sepulchre: Comparative perspectives. *Tulane European and Civil Law Forum*, 29, 131–160.
- Sweden's Data Protection Authority. (2020). *Decision regarding Google LLC's right to be forgotten obligations (€7 million fine)*.
- Uniform Law Commission. (2015). *Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)*.