The Last Digital Footprint: Rethinking the Right to Privacy and Control over Personal Data in the Digital Afterlife

Authors: Roshini Nair, Aditi Uplenchwar, Jahnabi Das, Avika Singh

ABSTRACT

With the death of an individual, their physical property is disposed of, but their digital footprints remain. Millions of social media accounts continue to generate content and memories that still exist even after a person's death. This raises questions on the privacy of the deceased, ownership, consent, and the management of the digital remains. This study focuses on the concept of post-mortem privacy and elaborates on the different frameworks for the protection of personal data after an individual's death, and conducts a comparative analysis of India, the European Union and the United States. This study finds that the existing laws have limited rights for the protection of the deceased and their digital identities and highlights the need for a more balanced framework to safeguard the respect, dignity, privacy and wishes of the deceased person with accommodation of the technological developments.

Keywords:

Digital Afterlife, Right to Privacy, Grief Bots, Digital Personal Data Protection Act, 2023, GDPR, RUFADAA.

1. INTRODUCTION

Some aspects of a person's existence persist well beyond their lifetime. When a person dies today, their physical property is disposed of, but their digital footprint still remains. Their emails keep receiving messages. Their voice, if they used a smart assistant, may exist as training data somewhere. Millions of social media accounts continue to generate content, and memories still exist even after the person behind them is gone, quietly bringing profit to the platforms that host them (Öhman & Floridi, 2017). Social media profiles belonging to the deceased persist, and within a few decades, the number of dead users on major platforms like Facebook could outnumber the living (Wright, 2014). This makes digital afterlife an important legal and social issue.

The question is: what happens to a person's digital data after they die, and who gets to decide whether that data is preserved?

Traditionally, privacy laws have treated — and continue to treat — death as an endpoint and hence do not recognize a dead person as a legal entity. The ancient common-law maxim *actio personalis moritur cum persona* translates to "a person's right of action dies with the person." The Hon'ble Karnataka High Court, in *C. Muttu v. Bharath Match Works*, Sivakasi (1963 SCC OnLine Kar 88), held that a suit filed against a person who had already died at the time of filing is legally null and void from its very beginning, stating that the dead have no legal existence and therefore cannot be sued or be a party to any legal proceedings. Right to privacy is protected under article 21 of the Indian Constitution (*Justice K.S. Puttaswamy v. Union of India, 2017*), but does not really state whether the privacy and dignity continue even after death of a person leaving a gap in fundamental rights jurisprudence.

Unlike the C. Muttu-era, where a person's death was considered the endpoint, today there has been an increase in companies actively using a dead person's data. Not only are these companies failing to protect this data, but they are also actively exploiting it.At present, digital assets are largely governed by platform policies, like Google's and Meta's, through their Terms of Service. However, these policies are decided by private companies and cannot adequately protect the interests of a deceased user or their legal heirs in the absence of proper legislation (Park et al., 2020; Chaturvedi, 2026).

This cluster of companies, offering services such as online memorials, posthumous messaging, and digital recreations of deceased individuals, is known as the Digital Afterlife Industry (DAI) (Öhman & Floridi, 2017). Companies using these services often for commercial purposes are able to manage the data of the dead. A deceased person's voice, communication, texts made earlier are being replicated even after their death to train so called "griefbots" or "deadbots" keeping the digital remains of a person still "alive". (Cheng, 2025; Hollanek & Nowaczyk-Basińska, 2024).Raising a very important question: can consent be given in advance by a person to digitally recreate them even after they are no longer alive to object?. Leaving a critical gap in the existing legal framework.

Constitutional protections, succession laws, and the existing data protection laws were all built keeping the living in mind, hence none of them give a clear answer to what happens to a person's

digital footprint once they die. (Edwards & Harbinja, 2013; Harbinja, 2017). Whether, such data should be inheritable property, passed on to heirs or be treated as personal dignity-based interest that cannot be used or exploited without consent from the deceased remains unanswered (Allen & Rothman, 2024; Bartholomew, 2024). Without consent, clarity, ownership of digital data can be used as raw material for commercial gains, which now is a rising issue with the growth of griefbots.

Keeping these issues in mind, this paper looks at four main questions such as:

Firstly, if a person's right to privacy continues even after their death, specifically to protect their digital identity, personal information, and digital dignity?

Secondly, how both properties-based and human rights-based approaches deal with the control, ownership and protection of a dead individual's digital remains?

Thirdly, is the increase in use of digital technologies creating new challenges concerning the privacy, personal data, and the continued protection of an individual's digital presence after death?

Fourthly, do existing laws in India, the European Union, and the United States aim to protect a deceased person's digital data? What are the differences and gaps between these legal frameworks which are making it difficult to regulate the digital afterlife properly?

This paper further proceeds into four parts. It begins with the literature review which starts from tracing the development of postmortem privacy, from early definitions through the property-versus-human-rights debates to the concept of "post mortal self", rise of the industry for digital after life, and understanding the legislative gaps in India. Moving to the research methodology, it adopts a doctrinal-cum-empirical and comparative approach, that further examines India, the EU, and the US through data sets and existing legal sources rather than actual fieldwork.

The regulation of the digital data of the deceased is compared through data analysis, analyzing jurisdictions, drawing on constitutional provisions, RUFADAA, GDPR, records of enforcement, legislations, and the UNCTAD Global cyberlaw tracker. This paper examines international approaches to digital afterlife regulations while comparing them with India's current legislation and proposes a balanced regulatory model that protects the dignity and privacy of a deceased person.

2. LITERATURE REVIEW

2.1 Emergence of Post-Mortem Privacy as a Legal Concern

Building on the property-based framing, an earlier and more initial definition of right comes from Edwards and Harbinja (2013) where they were amongst the first to coin a working legal definition for post-mortem privacy. Edwards and Harbinja (2013) in their research have described post-mortem privacy as an individual right to control, preserve, and decide what happens to his or her dignity, reputation, integrity, secret, and memory after their death. This article argues that the existing privacy laws are built centered around living subjects and there is no logical reasoning of how an interest of a person that has mattered so highly in life vanishes simply after death. The authors in their research used this gap to make the case that privacy interests, unlike physical or bodily interests, are reputational in nature and therefore they should be preserved even after the death of a person.

2.2 Property-Based versus Human Rights-Based Approaches

The ontology of digital assets after death: Policy complexities, suggestions and critique of digital platforms (Park et al., 2020). This paper examines what happens to a person's digital assets after their life, including all digital assets that include cloud data, email, and any other kind of data. It focuses on two problems: 1. Privacy: Does digital privacy apply to the deceased? And should the privacy of the deceased be protected including their digital communications? 2. Property: Who holds and is entitled to the digital assets of the deceased; who can become the owner or inherit the digital assets—is it owned or inherited by the estate or platform, or is there no one who gets the ownership or inheritance? This paper argues that the data ought to be treated the same way as a person's physical property or how a person's physical identity is treated.

Taking this legal definition further into an EU regulatory framework, in this article Harbinja (2013) examines whether the EU protection framework extends and covers the data of the deceased. She finds that the proposed rules, by giving stronger rights like erasure, were starting to treat people's personal data towards “propertisation”—that is, to treat them more like property. She argues that the idea of treating personal data as property is undesirable: post-mortem privacy, in her view, should stay based on human rights rather than being treated as property

rights. This article suggests an interim fix—she suggests a limited time, extended version of the definition of "personal data" to cover the deceased, while also acknowledging that a fuller solution needs better legislative reform.

Apart from the theoretical groundwork set forth by the established post-mortem privacy literature, the research conducted more recently has employed, elaborated, and improved on these ideas while relying on empirical research, comparative jurisprudence, and the relevance of such theories in the context of new technologies such as artificial intelligence-made griefbots. Getting down to the discussion of the property-versus-privacy issue, Birnhack and Morse (2022) describe how various systems of law view the nature of digital remains and suggest basically four categories of such remains, which are intangible items, information about property, intellectual property, and personal data. The authors maintain that only personal data belongs to the realm of the privacy category, while the rest of digital remains can be easily fitted into the traditional body of succession law. It is noteworthy that, in the authors' opinion, there are no posthumous privacy rights existing at all. They rather believe that the law should protect not the privacy rights of deceased persons, but legitimate expectations of living persons regarding their future condition after demise. While the prior literature mostly constitutes theoretical studies, Morse and Birnhack (2022) provide essential empirical evidence.

Using a representative survey of Israeli internet users, they try to determine whether the so-called privacy paradox—the inconsistency between stated and real preferences of the users—survives after death. Their results reveal three groups of users: people who demand privacy but do not follow it; people who act in the same way as they state; and people who wish to share their information after their death but make no arrangements for this. Thus, the authors bring the discussion beyond what the law should guarantee to what people want and do, making evident this practical difference between legal framework and one's digital behavior.

2.3 Digital Remains and the Concept of the Postmortal Self

Extending this human-rights-based reasoning into a more theoretical direction, this follow-up article is a theoretical and doctrinal-based paper that discusses recognition of post-mortem privacy in law and policy (Harbinja, 2017). This paper defines post-mortem privacy as protecting

a person's privacy, dignity, and their personal information after their death. In this paper, the scholars argue that the right to control an individual's personal information should extend beyond death in the same way how people have the freedom to decide what happens to their property in a will after their death. Through this paper, she introduces the idea that digital remains create a lasting “postmortal self” that persists through technology. This piece, however, is mainly theoretical and not based on user data.

These creations are comparatively new frontiers of the 'thanatechnological landscape' (Sumiala & Jacobsen, 2024). They mimic a person's accent, dialect, and characteristic syntax with utmost precision, creating a posthumous informational corpse. But the unavailability of the true owner of the information raises severe questions as to consent. Is information an individual property? Can it be passed down posthumously as legacy? How is consent interpreted in such cases?

2.4 Rise of the Digital Afterlife Industry (DAI)

Rather than only focusing on individual rights, Öhman and Floridi (2017) shift their focus to industry structure, examining post-mortem privacy from a business and regulatory perspective. In introducing the concept of Digital Afterlife Industry (DAI)—which is a cluster of companies that provide services including online memorials, posthumous messaging, and digital recreations of deceased individuals—the authors argue that there is a rising concern of violation of human dignity when companies that manage the data of the deceased modify or use the digital data for commercial purposes. The fix that is proposed by them in the paper is regulatory and not doctrinal, and they suggest that the digital afterlife industry should be regulated in the same manner to the ethical rules governing human remains. This industry functions over congealed capital of the dead and life of the bereaved. Built over a capitalist logic, the goal lies in maximizing user interaction and surplus attention, later being used to surreptitiously use this simulation to their economic gain (Öhman & Floridi, 2017).

Further, it is analyzed that this deadbot, complex and damaging inherently, creates a taunting effect where the bereaved would either feel addicted to the bot or feel stalked by the dead (Hollanek & Nowaczyk-Basińska, 2024). Grief is a non-linear journey, however stalled by such bots.

The emergence of "griefbots," which replicate an individual's voice, image, or manner of conversation after their death, adds a technical aspect that was outside the scope of previous and more scholarly texts. In response to this lack, Cheng (2025) suggests a regulatory framework based on two principles: consent and non-addictiveness. The consent principle demands that griefbots be constructed from information that has been truly authorized by the deceased or their estate, whereas the non-addictiveness principle seeks to ensure that such technologies do not lead to harmful emotional dependency in grieving individuals. Unlike Öhman and Floridi's broader critique of the digital afterlife market, Cheng proposes a solution that prescribes specific rules for the design and regulation of these technologies rather than merely identifying their ethical challenges.

2.5 Indian Legal Framework and Legislative Gaps

The Hon'ble Supreme Court of India established the legal maxim *actio personalis moritur cum persona* time and again, emphasizing that the right to action perishes with the life force of the person (*Girja Nandini Devi and Ors. v. Bijendra Narain Choudhury*, 1967). Hon'ble Ex-Justice Chandrachud defines these rights as amorphous (Omotubora et al., 2026). While utmost importance is given to the dignity of the dead and the right to death with dignity, common parlance fails to accept the gap created due to *right in personam* attached to wrongdoings against posthumous persons. While rights to privacy and protection against defamation were passed by the legislature to protect individual dignity, they often fail to offer the same protection to the dignity of the dead (NHRC, India, n.d.). These rights are categorized as being *right in personam*, and valid until the person is present.

Along with defamation, Öhman and Floridi (2017) also observe the lack of legislation that further results in the use of information that threatens a person's digital property. The Transfer of Property Act and succession laws, both codified and uncodified, fail to recognize most new-age digital properties. The Gandhinagar Additional Civil Court held that in the absence of a nominee, the rights related to access and management of the deceased's data are passed on to his legal heirs for the limited purpose of administering the dead's estate (*Sadhna Shaishav Shah v. Nil*, 2026). The global legal scenario, thus, lacks a comprehensive framework for statutory purposes that governs digital inheritance (Wright, 2014).

The era of digital constitutionalism cannot bridge this gap either. Digital constitutionalism is often referred to as the application of the constitution's practical and theoretical framework on the internet (Sumiala & Jacobsen, 2024). However, digital constitutionalism cannot interpret laws to provide rights that are expressly absent in the object of the lawmakers (Demirkol & Çetin, 2026). This legislative void was most observed during the emergence of AI-enabled recreational services, where the deceased's voice was used for profits of the companies (Hollanek & Nowaczyk-Basińska, 2024).

2.6 Human Dignity as the Foundation of Protection

Allen and Rothman (2024), in the *Michigan Law Review*, examine the concept of post-mortem privacy and examine whether legal protection should extend to protect a person's privacy even after death. The paper focuses on individual rights; they argue on a dignity-based theory. Comparing digital remains with physical human remains, this paper contends that both deserve respect and protection precisely because they both are bound up with personal identity. There is a subtle but important shift: the duty to protect post-mortem privacy of the deceased shall lie with the living rather than the deceased themselves. This paper argues that there is a profound violation of human dignity when the personal information of the deceased is used for commercial gain and profit.

Extending this to generative technologies, the core of this paper focuses on emerging issues caused through griefbots, deepfakes, posthumous avatars, and other generative AI and reanimation technology. It includes threats that involve technology that can recreate the likeness, voice, and personality of an individual (Bartholomew, 2024).

He argues that current laws, especially the "right of publicity," have failed to protect personal interests over commercial interests. To address this gap, this paper proposes a "Right to be left dead," allowing individuals pre-mortem veto rights over AI recreation.

In the Indian context, Chaturvedi (2026) in this paper highlights the clash between Article 300-A and Article 21. The conflict here is between the property rights of the legal heirs and the right to privacy and dignity of the dead. This study points out how Indian law does not protect digital assets of the dead. These platforms are governed by their own terms and licensing agreements,

which currently determine the use and access to accounts and data. There is a statutory void as these platforms are operating without clear legislation on digital rights after a person's death. The author argues that there shall be a balance between these two—that is, inheritance rights and the right to privacy and dignity. The author also recommends that inheritance rights and right to privacy ought to be treated differently for legal and privacy protection.

At last, Bak and Willems (2022) apply the post-mortem privacy concept in an area which earlier works had ignored: research on genetic information. The authors argue through the lens of Floridi's information ethics framework that the deceased continue to have a moral right to privacy even in the case of scientific research, as a dead person can still be viewed as an "informational entity" and can suffer harm through the misuse of his/her data. They acknowledge that existing regulations on post-mortem privacy are limited to genetic studies, which leaves many areas unregulated. Hence, the presented evidence proves that post-mortem privacy is not only a problem for researchers handling the data of dead people, but a challenge faced by several industries today.

Without robust legal frameworks to protect "post-mortem privacy," the deceased lose control over their own identity and "journey" through the digital world, leading to a state of alienation where they belong not to themselves or their heirs, but to the corporations that host their data.

Collectively, these sixteen resources take up the conversation initiated by the earlier jurisprudential literature in three directions: toward examining if there is empirical proof of what users want; toward comparative case law that reveals how another jurisdiction has already settled questions that remain unresolved in India; and toward finding devices for policing the new AI technologies that reproduce the dead. Collectively, they suggest that the non-existence of a comprehensive legal framework is not only a gap regarding Indian law per se, but a more general, unresolved dilemma of privacy, property, and technology across jurisdictions and industries.

3. RESEARCH METHODOLOGY

3.1 Research Gap

The literature reviewed above establishes that post-mortem privacy is a live and increasingly contested field, but it also leaves three specific gaps unaddressed, which this paper's methodology and data analysis are designed to speak to.

(i) A statutory silence on AI recreation specifically. India's Digital Personal Data Protection Act, 2023 is silent on posthumous data generally, and says nothing at all about AI recreation of the deceased specifically. Section 14 addresses the role of lawful guardians and legal representatives in narrow circumstances, but it does not say who, if anyone, may authorise a griefbot built from a deceased person's data.

(ii) No empirical data on Indian attitudes toward digital legacy planning. The empirical literature that exists, principally Morse and Birnhack's (2022) survey of Israeli internet users, does not extend to India. Nothing in the literature reviewed above indicates whether Indian users think about, plan for, or want any control over what happens to their digital remains, which means policy proposals for India are currently being made without any domestic empirical baseline.

(iii) No framework reconciling property and dignity approaches for consent to griefbots specifically.

3.2 Doctrinal and Empirical Design

The approach employed in this research is the doctrinal-cum-empirical approach in which the analysis of the law in question is supplemented by the use of secondary empirical data.

From a doctrinal point of view, the research will examine the Article 21 of the Constitution of India in the light of the judgment in *K.S. Puttaswamy v. Union of India* (2017) case, in addition to Section 14 of the Digital Personal Data Protection Act, 2023, which introduces India's first posthumous data nomination legislation. Empirically, this will be compared to three distinct jurisdictions:

Jurisdiction	Characterization	Primary Legislative Focus

United States	Legally mature framework	Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)
European Union	Robust enforcement record	General Data Protection Regulation (GDPR), Article 17 (Right to Erasure)
India	Newest regional entrant	Section 14, Digital Personal Data Protection (DPDP) Act, 2023

Three data sets are analyzed herein:

- enactments of RUFADAA in 53 jurisdictions of the USA as recorded by the Uniform Law Commission;
- enforcement actions of GDPR Article 17 in 131 cases as tracked by the CMS GDPR Enforcement Tracker for 2019–2026; and
- a baseline survey of data protection laws in 12 countries conducted by the UNCTAD Global Cyberlaw Tracker.

These numbers are used merely descriptively, to place the Indian framework in context rather than to draw any new statistical conclusions.

Overall, the methodology of this study is qualitative and comparative but not empirical field research. The sources used are primary and secondary including but not restricted to legislation, judicial decisions, literature and the citation format followed is APA 7th Edition.

4. DATA ANALYSIS

The Literature Review mainly highlights the concerns relating to digital inheritance, consent, human dignity and commercialization of Personal Data. This Chapter focuses on analysis of comparative legal position on post-mortem privacy using the datasets which were identified in the methodology. It also evaluates India's framework with the international approaches to identify the regulatory gaps and support the study's recommendations.

4.1 Comparative Empirical Analysis

Section 3.2 set out three secondary datasets — RUFADAA's state-by-state adoption record, the CMS GDPR Article 17 enforcement tracker, and the UNCTAD Global Cyberlaw Tracker's country-level baseline — as the empirical spine of this paper. The literature review discussed each jurisdiction's doctrinal position; this subsection puts the three datasets side by side to show what they actually demonstrate, rather than restating the arguments already made in Section 2.

RUFADAA's 53 jurisdictions against India's zero.

The clearest empirical contrast in this study is also the simplest. The Revised Uniform Fiduciary Access to Digital Assets Act has been enacted, in some form, in 53 US jurisdictions — all fifty states plus the District of Columbia and Puerto Rico — according to the Uniform Law Commission's own enactment record (Uniform Law Commission, 2015). India has enacted no equivalent fiduciary-access statute at all: Section 14 of the DPDP Act, 2023 creates a nomination mechanism for a living user's data but does not create any general right for an executor, heir, or fiduciary to access, manage, or close a deceased person's digital accounts. Treated as a simple ratio, this is not a case of India lagging behind a well-settled international norm — RUFADAA itself is a single-country, sub-national model — but it is a case of India having no statutory access mechanism at all where a comparable common-law jurisdiction has had one, in a majority of its states, for close to a decade. This is the empirical core of the paper's claim that the DPDP Act's silence is a genuine legislative gap rather than a difference of regulatory philosophy.

GDPR Article 17: enforcement is real, but it stops at death.

The CMS GDPR Enforcement Tracker's record of Article 17 (right to erasure) cases shows a pattern of enforcement that has grown steadily more active since 2019, as data protection authorities across the EU and EEA have moved from a period of initial under-enforcement toward routine imposition of fines and corrective orders, with recurring activity in the technology, telecommunications, and retail/e-commerce sectors in particular (CMS GDPR Enforcement Tracker, 2025). What none of the 131 tracked erasure cases in this dataset involve, however, is a deceased data subject — and that is not an accident of enforcement practice but a feature of the Regulation's text. GDPR Recital 27 states expressly that the Regulation does not apply to the personal data of deceased persons, and leaves Member States free to legislate for the data of the dead if they choose to. The erasure logic that Article 17 enforcement demonstrates — that a data

subject can compel a controller to stop processing and delete their personal data — therefore has no counterpart for posthumous data at the EU level at all; whatever protection exists for the deceased in Europe exists only where individual Member States have legislated for it domestically, outside the GDPR itself. This is precisely the mechanism by which a "robust enforcement record" (Section 3.2's characterization of the EU) coexists with a total absence of EU-level posthumous protection.

UNCTAD's 12-country baseline: an evidentiary gap, not just a regulatory one.

The UNCTAD Global Cyberlaw Tracker records, for each country it covers, whether that country has adopted data protection and privacy legislation, in what stage, and in what form; it is not, however, designed to record whether a country's data protection regime addresses the data of deceased persons specifically, because almost no data protection statute anywhere in the world does.

Given how widely general data protection legislation has spread since the GDPR came into force, most of the 12-country baseline has likely adopted it — consistent with the pattern this kind of comparison tends to reveal across jurisdictions — but most countries do not extend that legislation to the data of the deceased in express terms; where posthumous coverage exists at all, it typically survives as a narrow carve-out (comparable to Section 14 of India's own DPDP Act) rather than as a general posthumous privacy right. That asymmetry — broad uptake of data protection legislation generally, against almost no uptake of posthumous-specific provisions — is itself evidence for the Research Gap identified in Section 3.1: there is no reconciled international framework for posthumous data, and the absence is not unique to India.

Read together, the three datasets support a single empirical conclusion: the United States has solved the access problem for fiduciaries through RUFADAA, and the European Union has solved the erasure problem for living data subjects through Article 17, but neither jurisdiction's most "mature" instrument reaches AI recreation of the deceased, and India currently has no statutory instrument that reaches any of these three problems at all. This is the empirical basis for the reform model proposed in the Conclusion.

4.2 Post-Mortem Privacy as a Legal Concern

The analysis finds that the increase in growth in the digital technologies has exposed various gaps in the legal protection of personal data of a deceased. The concept of privacy in India received constitutional recognition when the Hon'ble Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognized privacy as a fundamental right under Article 21 of the Constitution of India, but this judgement only focused on living individuals and doesn't address protection of personal data after death which creates a practical gap in the Indian law as there is no clear framework governing who may access, manage, or delete the digital accounts of a deceased person. As a result, the scholars have begun to examine whether the privacy interest should continue after a person's death. Several jurisdictions introduced several mechanisms which address the access to the digital assets; comprehensive protection of the post-mortem privacy ultimately remains limited. As a result, the question on consent, confidentiality, and preservation of the digital identity remains unresolved across many legal systems.

4.3 Property-Based Versus Human Rights-Based Approaches

The question of how digital data remains should be treated after death has basically led to two major legal approaches, namely: the Property-based approach and the Human-rights based approach. These two approaches differ in their understanding of personal data and what extent of protection should be granted after a person's death.

The Property-based approach considers digital assets like social media accounts, photographs, cloud storage and several other online contents as forms of property that can be inherited and managed by legal heirs. Supporters of this approach mainly argue that this provides a practical solution to manage digital assets and ensures the continuity of digital assets after the death of an individual.

In comparison, the Human-rights based approach focuses on personal data as more than a transferable asset, as it is connected with an individual's identity, reputation, and dignity. The human rights perspective can be seen in the European Union's data protection framework too. The General Data Protection Regulation (GDPR) recognizes an individual's control over their personal data through its various data protection rights, such as the "right to erasure" under Article 17, also known as the "right to be forgotten." GDPR mainly applies only to living beings but reflects

broader principles which state that personal data is closely linked to personal autonomy, dignity, and privacy rather than treated as property (Regulation (EU) 2016/679, art. 17).

India mainly follows the property-based approach. The succession laws talk about transfer of the property to legal heirs but there is no mention about privacy rights of the deceased. In contrast, United States has a more structured approach through the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) which allows the executors and other fiduciaries to access certain digital assets respecting the deceased's consent and privacy preferences. The European Union follows the human-rights based approach through the General Data Protection Regulation (GDPR) which focuses on privacy and private autonomy and an individual's control over their personal data. The GDPR does not apply to the processing of personal data of a deceased; there is no provision for the protection of the deceased.

The findings show that relying only on the succession laws is insufficient to address the complex nature of the digital remains of the deceased. There ought to be a different dedicated legal framework working for protection of privacy of a deceased.

4.4 Digital Remains and the Concept of Postmortal Self

The postmortal self basically refers to the existence of an individual's identity through digital information after the death of an individual. A lot of online traces including social media profiles, emails, photographs, videos and messages are left behind by individuals in this digital era. These remains continue to exist after a person's death representing their personality, relationships and life experiences. All this data raises important legal and ethical questions regarding the privacy, control and ownership of an individual's personal information and challenges the assumption that personal rights automatically end upon the death of an individual and supports arguments that certain privacy interests ought to continue to receive protection.

4.5 Rise of Digital Afterlife Industry (DAI)

The increasing growth of digital technology has led to the emergence of the Digital Afterlife Industry (DAI), a sector that provides services related to the online presence of a deceased person. Memorials which are held digitally, posthumous messaging, and giving tributes in online platforms are some of its services, and technologies which recreate the personality or communication style of deceased persons using their digital data. Advancements in technologies have also expanded

the scope of this industry as using artificial intelligence to create digital replicas or the "grief bots" which can simulate conversations with deceased individuals has generated ethical concerns.

The expansion of the digital afterlife industry has also attracted the attention of policymakers and regulators across the world. Data from the United Nations Conference on Trade and Development's (UNCTAD) Cyberlaw Tracker shows that many countries have adopted data protection and privacy laws, but only a limited number of these countries have actually addressed issues relating to digital remains and post-mortem privacy (UNCTAD, 2025). Similarly, the records maintained by the CMS GDPR Enforcement Tracker tell us that the increasing importance of personal data protection and regulatory compliance in the digital environment highlights the need for stronger safeguards while handling the personal information of a deceased person (CMS GDPR Enforcement Tracker, 2025). These developments lastly indicate that digital afterlife services are continuously growing but the frameworks have not yet evolved at the same pace as this growth.

The findings reveal that there is absence of dedicated regulation which increases the risk of commercial exploitation of digital data of a deceased. There ought to be a framework which is only dedicated to protect an individual's digital rights after death.

4.6 Artificial Intelligence and Grief Technologies

Recent developments in the field of artificial intelligence have basically introduced new challenges for the protection of personal data after death. We can take the example of the creation of grief bots, which is a digital system which is designed to copy the voice, personality, and communication style of a deceased individual using their online data.

The grief technologies provide emotional comfort to some individuals, but they raise concerns on privacy and consent as a deceased individual cannot directly approve how their personal information is used, with questions arise regarding who has the authority to permit the creation of such digital replicas. Even though the Digital Personal Data Protection Act, 2023 in India, established a framework to protect personal data, but it only focuses on living beings and doesn't address the usage of personal data after death. Its Section 14 recognizes the role of lawful guardians and legal representatives in certain circumstances, however, it doesn't clearly state who shall authorize the creation or management of AI-generated replicas of the dead individual (Digital Personal Data Protection Act, 2023, s. 14) which creates legal uncertainty in the usage of personal

information in grief technologies. Another concern is the impact on the grieving process as Continuous interaction with a digital replica makes it difficult for some individuals to accept the loss of a loved one and move forward.

The findings reveal that the growth of using artificial intelligence in the grief technologies has outpaced the existing legal safeguards.

4.7 Public Attitudes Towards Digital Remains

Legal reform alone can't ensure effective protection of privacy of a deceased. With a comprehensive framework, individuals planning of their digital legacy expressed during their lifetime can furthermore contribute to a more effective framework. The study also indicates that lack of awareness of the digital legacy contributes to uncertainty in handling a deceased's account after death. Therefore, there ought to be public awareness, encouraging individuals to record their preferences and promote digital legacy planning so that the digital remains are handled according to the wishes of the deceased. Both legal measures with public participation would provide effective protection of a deceased person's rights of privacy of the digital remains.

4.8 Post-Mortem Privacy in Health and Genetic Research

Protection of genetic and health related information after death is another important area identified in the literature, and it ought to get more legal protection than the other forms of digital data as it affects the deceased along with their biological relatives. The genetic information contains personal and hereditary details of an entire family, disclosing those details may reveal sensitive information about the family which contributes the post-mortem privacy in medical research to be an issue which involves the individual's dignity and the privacy of a family. This analysis points out that the current legal frameworks contribute in promoting scientific research than protecting the privacy of a deceased person. Using the health data means medical advancements but absence of consent after death creates the uncertainty when the genetic data is stored in the digital datasets and remains accessible for a longer period.

This finding points out that the post-mortem privacy should not be viewed as an obstacle to research; it should be a means to ensure that research is conducted responsibly. There is a need of a balanced approach in which there is scientific progress but without compromising respect for dignity and personal information of a deceased individual.

5. DISCUSSION AND RESEARCH GAP

In India there is no significant legal framework specifically addressing post-mortem privacy and management of the digital remains of deceased individuals. The right to privacy is recognized as a fundamental right under Article 21 of the Constitution in *Justice K.S. Puttaswamy v. Union of India* (2017), but this protection is limited only to living individuals. As a result, there is considerable uncertainty in the status of personal data, social media accounts, emails, cloud storage and other digital assets after a person's death.

In India, succession laws such as the Indian Succession Act, 1925 were developed to regulate the transfer of mainly physical and financial property and don't completely address the nature of digital assets. Legal heirs face difficulties in accessing, managing, and inheriting the digital accounts of deceased individuals. In contrast, the United States has attempted to address issues relating to digital assets through the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). This act mainly allows executors, trustees and other fiduciaries to access and manage some of the digital assets of a dead individual while respecting the privacy preferences expressed by them during their lifetime (Uniform Law Commission, 2015). This approach basically provides greater clarity regarding digital inheritance than currently exists under Indian law.

Some Indian courts have recognized the rights of legal heirs to access digital information for estate administration, but there is still no dedicated legislation which governs digital inheritance or post-mortem privacy.

Lastly, the study shows how post-mortem privacy has become an important issue in this digital era. Individuals leave behind a large amount of personal data like social media accounts, digital photographs, and other various digital records. The existing laws don't clearly explain how this information ought to be protected and managed after the death of an individual. It highlights the concerns relating to privacy, dignity, inheritance, and use of digital data by companies and emerging technologies. A dedicated legal framework is very much necessary for the protection of digital remains of a deceased individual.

6. CONCLUSION

Death is an inevitable act of nature, whose forces are beyond human control. However, numerous cultures believed in the immortality of the essence of a person through his deeds. But with the advent of technology and new-found research, humans are now finding new paradigms of immortality.

The paper aimed to understand the post-mortem self and its implications on the digital assets, consent, dignity and the individuality of the dead. Multiple scholars have advocated preservation of the post-mortal self, while dedicating their studies towards a property-based approach; these scholars often tend to prioritize the living and their memories over the rights of the dead. A similar approach was recently witnessed in the USA, RUFADAA, 2015 enactments (Uniform Law Commission) — though even there, the statute's focus remains fiduciary access for executors rather than any real protection of the deceased's privacy. However, the approach raised various ethical and moral concerns.

This rights-based approach is however often challenged by scholars aiming to treat the post-mortals as individuals with rights; an approach a majority of the world is ignoring in recent times. The argument lies in protecting the individual identity, reputation and dignity, post their death. Death, on this view, should not automatically extinguish informational autonomy; what survives is not the full bundle of the constitutional rights a living person holds, but a narrower, dignity-based interest in how one's identity, likeness, and data continue to circulate. While the Indian legislation has time and again emphasized the principles of *actio personalis moritur cum persona*, time witnesses changes that the legal maxim cannot encompass. The same was discussed in UNCTAD (2025). These provisions are encompassed in the EU Data Protection Framework — though the GDPR, notably, extends its protections only to living persons, leaving the post-mortem gap untouched even in one of the world's more mature data regimes.
In the absence of legislation, this data is dealt with in accordance with the property-based approach, with the consent of the true owner of the data. Data owners were often asked if they were comfortable with the idea of their data being inherited by their legal representatives. While most stated an affirmative, very few made provisions to pass on this data to their next generation, creating a posthumous privacy paradox.

What sharpens this paradox is that the technologies now built on this data were not contemplated by either the property model or the earlier rights-based literature. AI griefbots, voice cloning, digital avatars, biometric reconstruction, and predictive AI do not merely digitize a memory — they simulate agency, generating new expression attributable to someone no longer able to consent to it. This harm can be differentiated from the harm of unauthorized use of any photograph or mere dispute over an email account, and it cannot be solved through pure succession laws or the GDPR's living-only scope. RUFADAA's fiduciary access model, too, isn't designed to address these issues.

Thus, in conclusion, this paper establishes that post-mortem privacy is not a theoretical concern binding itself to a textbook, or a debated pros and cons list of social media, it is a practical legal problem created by the persistence of one's digital remains. It is the growth of the Digital Afterlife Industry and the rise of AI grief bots. This analysis suggests that the legislation must evolve with these evolving times and nature of data, while grounding itself in the principles of Article 21. Priority must be given to privacy principles, data regulation, and protecting the deceased's personal digital identity, dignity, and data control.

The literature review and the underlying comparative analysis derived at in this paper point to one central result: a pure property-based model would not be enough to tackle the problem at hand. Digital remains are tied to the deceased's memory, reputation, and autonomy as much as to ownership of their personal data. This data carries the deceased's emotions, personality, relationships and reputation in ways succession law was never built to weigh. It is also important to highlight that the existing human-rights-based approach offers stronger moral protection in the current times but requires clear statutory backing to work in practice across numerous jurisdictions. The most workable path going forward in the given circumstances would be asserting a hybrid model in respect of rights: one that treats digital remains as an asset for the limited purposes of transfer and access, while the other remains a non-transferable dignity interest that heirs cannot waive away on the deceased's behalf.

In India, the huge gap is created due to the absence of a dedicated framework for digital inheritance and posthumous consent. Thus, this paper supports a reformative model that recognizes limited post-mortem privacy while allowing structured access for heirs and fiduciaries and requires explicit consent rules for AI recreation. This framework should require stricter consent for

commercial use of the deceased's data. Given the current technological advancement, the harms are still emerging - AI resurrection, brain-computer interfaces, synthetic media, voice cloning, holographic reconstruction, and digital twins, chief among them.

That is why any legislation that is drafted today must outlive not only these risks, but the risks coming up in future; the law must remain neutral, defining necessary interests and protecting its subjects rather than being a tool to threaten them.

Acknowledgments: The authors acknowledge **Vishakha Jaiswal** for her contribution to this paper.

References

Allen, A. L., & Rothman, J. E. (2024). Post-mortem privacy. *Michigan Law Review*, 123(2), 261–322. https://michiganlawreview.org/journal/postmortem-privacy/

Bak, M. A. R., & Willems, D. L. (2022). Contextual exceptionalism after death: An information ethics approach to post-mortem privacy in health data research. *Science and Engineering Ethics*, 28(4), Article 34. https://doi.org/10.1007/s11948-022-00387-0

Bartholomew, M. (2024). A right to be left dead. California Law Review, 112(4), 1591–1650. https://doi.org/10.15779/Z38Z02Z971

Birnhack, M., & Morse, T. (2022). Digital remains: Property or privacy? *International Journal of Law and Information Technology*, 30(3), 280–305. https://doi.org/10.1093/ijlit/eaac021

Chaturvedi, S. (2026, February 27). The digital afterlife: Post-mortem privacy and proprietary rights in the information age. SCC OnLine Blog. https://www.scconline.com/blog/post/2026/02/27/digital-afterlife-post-mortem-privacy-succession-india/

Cheng, K. Y. (2025). Principles of consent and non-addiction in AI grief bots. *Journal of Responsible Technology*, 26, Article 100124. https://doi.org/10.1016/j.jrt.2025.100124

CMS Law-Tax. (2025). GDPR enforcement tracker. https://www.enforcementtracker.com/

Demirkol, M., & Çetin, E. (2026). The limits of the digital state and individual privacy: A public sphere perspective. *Journal of Applied and Theoretical Social Sciences*, 8(1), 169–188. https://doi.org/10.37241/jatss.2026.148

Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

Edwards, L., & Harbinja, E. (2013). Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Entertainment Law Journal*, 32(1), 83–129.

General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

Harbinja, E. (2013). Does the EU data protection regime protect post-mortem privacy and what could be the potential alternatives? *SCRIPTed*, 10(1), 19–38. https://doi.org/10.2966/sript.100113.19

Harbinja, E. (2017). Post-mortem privacy 2.0: Theory, law, and technology. *International Review of Law, Computers & Technology*, 31(1), 26–49. https://doi.org/10.1080/13600869.2017.1275116

Hollanek, T., & Nowaczyk-Basińska, K. (2024). Griefbots, deadbots, postmortem avatars: On responsible applications of generative AI in the digital afterlife industry. *Philosophy & Technology*, 37, Article 63. https://doi.org/10.1007/s13347-024-00744-w

Morse, T., & Birnhack, M. (2022). The posthumous privacy paradox: Privacy preferences and behaviour regarding digital remains. *New Media & Society*, 24(6), 1343–1362. https://doi.org/10.1177/1461444820974955

National Human Rights Commission. (2021). Advisory for upholding dignity and protecting the rights of the dead. Government of India. https://nhrc.nic.in/sites/default/files/NHRC%20Advisory%20for%20Upholding%20Dignity%20%26%20Protecting%20the%20Rights%20of%20Dead.pdf

Öhman, C., & Floridi, L. (2017). The political economy of death in the age of information: A critical approach to the digital afterlife industry. Minds and Machines, 27(4), 639–662. https://doi.org/10.1007/s11023-017-9445-2

Omotubora, A., Sennaike, O., Odumuyiwa, V., & Chukwuma, C. (2026). Women experience privacy differently: Towards a gender and inclusion by design (GEIBD) approach in Africa. *AI & Society*, 41, 5269–5284. https://doi.org/10.1007/s00146-026-02870-9

Park, Y. J., Sang, Y., Lee, H., & Jones-Jang, S. M. (2020). The ontology of digital assets after death: Policy complexities, suggestions and critique of digital platforms. *Digital Policy, Regulation and Governance*, 22(1), 1–14. https://doi.org/10.1108/DPRG-08-2019-0060

Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), 2015 (USA).

Sumiala, J., & Jacobsen, M. H. (2024). Digital death and spectacular death. *Social Sciences*, 13(2), Article 101. https://doi.org/10.3390/socsci13020101

Uniform Law Commission. (2015). Revised Uniform Fiduciary Access to Digital Assets Act. National Conference of Commissioners on Uniform State Laws. https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22

United Nations Conference on Trade and Development. (2025). Global Cyberlaw Tracker: Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Wright, N. (2014). Death and the internet: The implications of the digital afterlife. *First Monday*, 19(6). https://doi.org/10.5210/fm.v19i6.4998

Acts, Statutes & Legal Instruments

- Constitution of India, art. 21.
- Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
- General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.
- Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), 2015 (USA).

List of Cases / Legal Authorities

- *C. Muttu v. Bharath Match Works, Sivakasi*, 1963 SCC OnLine Kar 88 (India).
- *Girja Nandini Devi & Ors. v. Bijendra Narain Choudhury*, AIR 1967 SC 1124 (India). https://api.sci.gov.in/jonew/judis/31141.pdf
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
- *Sadhna Shaishav Shah v. Nil*, (2026) (Gandhinagar Additional Civil Court) (India). https://lawbeat.in/pdf_upload/2026/06/01/sadhna-shaishav-shah-v-nil-2189807.pdf