



## **THE LAST DIGITAL FOOTPRINT: RETHINKING THE RIGHT TO PRIVACY AND CONTROL OVER PERSONAL DATA IN THE DIGITAL AFTERLIFE AND RIGHTS IN THESE DIGITAL TIMES**

**Authors:** ANANYA SONI, PINKI GUPTA, RENUKA DEVI A, SALEENA ASHRAF

### **ABSTRACT**

Social media accounts and other digital things like cloud storage or emails keep going even after someone dies. This creates questions around privacy and who gets to control all of them. In India, there is no clear set of rules yet for handling what happens to these digital remains. People might want to access them or delete them, but it is not straightforward who has the right to decide.

The paper looks at how the rights of the person who passed away might clash with what their family wants or what companies allow. It also considers third parties involved. The approach uses doctrinal methods and compares things to laws in other places. Article 21 of the Constitution comes up along with the IT Act and the newer data protection law from 2023. Some court cases are mentioned too. On the side of comparison, there are rules like RUFADAA in the US and approaches in Europe, including France and Germany. It seems the current Indian position is a bit scattered. Succession laws might cover some assets, but privacy concerns and contracts with service providers can block full access. I think that means heirs do not always get unrestricted control. A mixed solution is suggested where digital remains could be treated as part of an estate for inheritance purposes. At the same time, there would be limits to protect dignity and privacy. This leads to a framework with things like instructions in a will, a person appointed to handle digital matters and rules that limit access based on purpose. There are also ideas around rights to close accounts or keep some identity intact. India probably needs changes to a few laws to make this work better overall. Some parts feel connected, but not every issue gets fully resolved in one go.

**Keywords:** Digital footprint; digital remains; digital afterlife; postmortem privacy; digital succession; Article 21; DPDP Act 2023;



## 1. INTRODUCTION

The death of a person does not always mean the end of their presence. Social media profiles, emails, picture files stored in the cloud, online accounts, subscriptions and other forms of information can still be around long after the person has passed away. These digital traces, often called footprints or digital remains, bring up legal questions about who can access, manage, keep, transfer or remove them after death. As more people rely on platforms, the traditional idea of what stays after a person dies has changed. This has led to a need to look at the status of these digital parts of a person's life.

Digital remains are not about things that have monetary value. They can include personal messages, pictures, memories, financial details and other private information. Managing these after someone dies can involve people who have different interests. Family members, heirs, service providers and others might want to access accounts for reasons like inheritance, remembering or practical needs. This access can also go against the wishes of the person who died, their privacy, their freedom, their dignity and the way they wanted their information handled. This creates a question about whether old ideas about property and who gets what are enough to handle digital remains or if a new legal approach is needed.

The rise of intelligence has made the idea of a digital afterlife even bigger. AI tools can now create parts of a person's identity after they die, like their look, voice, ways of acting or how they speak. Even though these tools might help with remembering and honouring a person, they also raise questions about permission, respect, identity, privacy who owns the parts and the chance of being used for profit. The ability to make a copy of a person after death challenges ideas about what it means to be alive, how a person's identity is connected to their body and how they are represented in the digital world.

These issues are especially important in India, where there is no one, full legal system designed to deal with digital remains and the digital afterlife. Different parts of the problem might connect to rights, laws about technology, data protection laws, laws about creative works, laws about passing on property, contracts and rules about privacy and respect. These rules were not made to handle the complicated questions about controlling and treating a person's digital life after they die. The legal situation is therefore not clear, especially when it comes to the rights of family and heirs to keep information safe and to use a person's digital identity with new technologies.



In this situation, the existing research gives ideas about the legal and ethical sides of digital footprints, digital remains and the digital afterlife. Experts have looked at topics like keeping privacy after death passing on things, who owns digital things, respect for a person and the ethical issues of keeping or making a copy of a person's identity. The research also shows that there is still confusion about how well these ideas fit into the Indian legal system. A full look at the research is needed to understand how these ideas developed, find where people agree or disagree and see what legal problems have not been solved yet.

This study looks at the research on footprints, digital remains and the digital afterlife from legal and ethical points of view, focusing especially on privacy, respect, ownership, passing on things and controlling what happens to a person's digital identity after they die. By looking at the research, the review wants to find the limits of current legal ways and show where more study is needed, especially in India.

## **2. LITERATURE REVIEW**

In recent years, legal and ethical scholars including Öhman and Floridi (2018), Edwards and Harbinja (2013), and Lingel (2013) have explored digital footprints, digital remains, and the digital afterlife from a legal and ethical standpoint. Social media accounts, cloud storage accounts, email addresses, and AI-powered memorial technologies that preserve an individual's identity even after death raise many concerns about privacy, dignity, succession, and personal data control. Should digital data be deleted right after a person's death, or should we preserve it, and how can it hinder the present generation as well as the generation that ceases to exist?

From a legal perspective, digital remains present a particular challenge because existing law related to privacy, succession, property, and personal data was largely developed without taking into account digital remains. In India, the legal position regarding ownership, control, access, and protection of a deceased person's digital remains is fragmented. This literature analysis therefore examines existing laws and academic research papers concerning the afterlife of digital footprints of the deceased, addresses the specific gaps in Indian law and assesses whether the present legal framework adequately addresses the rights and interests arising from a person's digital existence after death. To identify the particular legal deficit in India, this literature analysis concentrates on the current research on these subjects.



## DIGITAL FOOTPRINT AND DIGITAL AFTERLIFE

Digital remains are not something that can be handled through regular property law by itself. There are new complications that come up with online data and accounts. I think that is why the usual rules do not cover everything. Some of the details still feel a little off, though. For example, according to Öhman and Floridi (2018) and other authors, the digital life after death sector needs to be regulated ethically since it may exploit the dead in a way that violates human dignity. They also suggest that digital remains should be recognised as "informational corpses." It also includes the contention that artificial intelligence-powered deathbots have the potential to trivialise the grief and mourning process and distort identity, raising ethical concerns for both the living relatives and the departed.

Other scholars, such as Kaushal (2026), concentrate on the conceptual difficulty of attempting to classify digital remains under conventional legal categories. The authors highlight the shortcomings of succession models by pointing out that digital remains are difficult to classify as either property or privacy. Although this criticism is useful in highlighting the shortcomings of conventional legal classifications, the classificatory approach might not adequately address the moral dilemmas surrounding the use of a deceased person's data. By proving that data must be protected in some way after a person passes away, Harbinja's work also adds to the conversation around post-mortem data protection. Her work is significant because it highlights the connection between data regulation and post-mortem dignity, but it is challenging to turn this normative position into particular legislation. Edwards, L., & Harbinja, E. (2013). Lingel contends in a related study that although digital footprints can be used to honour the dead, there are issues with accessibility, visibility, and control related to the deceased's digital legacy (Lingel, 2013).

Taken together, this body of literature reveals two connected fault lines rather than a single debate. The first is definitional: scholars disagree on whether digital remains are best understood as property, as privacy interests, or as something that resists both categories, and this uncertainty is what leaves succession law unable to fully absorb them. The second is normative: even where classification is set aside, authors such as Öhman and Floridi (2018) and Morris and Brubaker (2024) show that AI-driven recreation of the deceased raises independent concerns about dignity, consent, and exploitation that a property-based or a purely privacy-based framework cannot resolve on its own. Read together, the literature therefore points not to a single missing rule but to the need for a framework that can hold administrative,



dignitary, and technological concerns at the same time, a gap this paper returns to in the Research Gap section below.

## **SOCIAL MEDIA, PRIVACY, AND DIGITAL CONTROL**

Technological advancements have made it simple for people to gather and disseminate their personal data, which may persist even after they pass away. In the digital age, this has generated a lot of legal discussion concerning privacy, control, and access to personal data after death. There is existing research in the Indian context to conclude that postmortem privacy and digital estate are not addressed by the current legal framework. Mali and Prakash (2019) have claimed that India's succession rules have not been revised to include digital properties. By placing informational privacy under the right to privacy established in the *K.S. Puttaswamy v. Union of India* (2017) case, Kaur and Nath (2025) provide a significant constitutional analysis of informational privacy. The idea that control over information is a fundamental component of privacy under Article 21 is supported by the reasoning given by Kaur and Nath (2025). Although Kaur and Nath's (2025) discussion does not focus on departed people, it can serve as a constitutional foundation for applying privacy reasoning to digital assets that have passed away. From this body of literature, one can see that there is not only fragmentation within the legal system, but there is also a possibility of an actual conflict of interests arising due to the nature of the law. While the principle of succession may be used by legal heirs to gain access to and manage their digital remains, the principle of privacy and data protection may provide grounds for withholding access to personal and sensitive information. On the other hand, issues of dignity and testamentary freedom may demand that the wishes of the deceased about the fate of his/her digital remains be taken into account.

## **REAL-WORLD EXTREMES OF POSTHUMOUS DIGITAL DATA**

The scholarly research done and actual examples prove that digital footprints after death can lead to repercussions beyond the areas of preservation, memorialization, and inheritance. The Roman Mazurenko chatbot serves as an example of the transformation of personal information such as messages, photos, etc., into an artificial personality and gives rise to questions regarding posthumous consent, the privacy of the person's personal correspondence, and the genuineness of messages sent from the dead person's alleged mouth (Morris & Brubaker, 2024). Likewise, the recreation of Nayeon, a dead seven-year-old girl, through VR helped her mom meet the digital avatar of her daughter; this incident provides an example of how digital cloning can impact personality rights, identity, dignity, and the emotional well-being of family members



(Boothe, 2022). Suharto's deepfake represents another way in which post-mortem identities can be transformed: during Indonesia's 2024 presidential election campaign, an AI-created video simulated the image and voice of Suharto in what seems to be a political message, showing how the identity of a dead public figure can be used for political persuasion and public memory manipulation (CNN, 2024). While these cases involve different uses of digital remains- a personal memento, immersive mourning, and political messaging altogether they illustrate how digital remains can be used to recreate new messages and influence beyond death. In other words, digital remains cannot only be considered an inheritable asset because their post-mortem use involves identity, dignity, vulnerability, reputation, public memory, and decision-making processes; the law needs to account not only for access and inheritance issues but also for consent, accuracy, purpose, and control involved in recreating and using a person's digital identity.

## **INDIAN LEGAL FRAMEWORK AND JUDICIAL DEVELOPMENTS**

The Indian legal system has advanced significantly since the historic decision of *K.S. Puttaswamy v. Union of India* (2017), in which the Indian Supreme Court declared that informational privacy is a crucial component of Article 21 of the Indian Constitution and acknowledged privacy as a basic right. But it's still unclear if any portion of the right endures after death. The Third Additional Senior Civil Judge of Gandhinagar, Gujarat, gave a significant ruling in May 2026. The judge decided that since the deceased's iPhone and iCloud data were a part of their estate, they were subject to succession regulations. The Court argued in its order for the issuance of Letters of Administration in favor of the deceased's legal heirs that heirs can administer the deceased's estate, even if it is digital in nature, and that privacy is a personal right that expires upon death. While the ruling does serve to recognise digital assets under succession law, there is a potential concern that the issue of privacy being erased upon death is not adequately addressed considering the relational nature of digital data, especially in cases where the digital information concerns both the deceased and living individuals. The Digital Personal Data Protection Act, 2023, together with the Digital Personal Data Protection Rules, 2025, establishes India's comprehensive statutory framework for digital personal data protection. By establishing the rights of data principals and the obligations of data fiduciaries, the Act gives people more control over how their data is handled throughout their lives. However, it doesn't address digital succession, digital estate management after death, or privacy in death. Because of this, modern jurisprudence continues to hold that the Indian law of



succession, which was created with traditional and tangible forms of property in mind, is insufficient for digital assets.

### **3. RESEARCH GAP**

The existing literature confirms that digital footprints and the digital afterlife persist beyond death, and that this persistence raises overlapping concerns of privacy, dignity, succession, ownership, and control. However, these concerns have so far been examined in isolation: one strand of scholarship addresses digital remains as property or succession assets, a second addresses them through privacy and dignity, and a third largely outside the Indian context which addresses them through the ethics of AI-based recreation. No study identified in this review brings these three strands together into a single legal framework capable of allocating access among the competing claims of heirs, the deceased's residual dignity interests, third parties who appear in the data, and the platforms that hold it. In India specifically, this absence is compounded by the fact that succession law, privacy jurisprudence, and the Digital Personal Data Protection Act, 2023 have each been analysed separately, with little scholarly attention to how an heir's statutory duty to administer an estate under Sections 317–318 of the Indian Succession Act, 1925 can be reconciled with the extinguishment of privacy rights recognised in cases such as *Ruba Ahmed v. Hansal Mehta* (2022). This study addresses that gap by proposing an integrated, purpose-based framework, rather than a single new statute that reconciles the interests of the deceased, heirs, third parties, and digital service providers.

### **4. RESEARCH QUESTIONS**

1. How can digital remains be treated as property without undermining the deceased's dignity?
2. How do privacy norms including the protection available under article 21 of the Indian Constitution limit or enable heirs' access under existing succession law in India?
3. What balancing mechanisms do comparative regimes (e.g., RUFADAA in the US, GDPR-based frameworks in the EU, German inheritable-contract doctrine, and French postmortem directives) offer, and which of these are transferable to India?



## 5. RESEARCH OBJECTIVES

In pursuit of the research questions outlined above, this study is guided by the following objectives:

1. To examine the conceptual foundations of digital remains in Indian law
2. To map the doctrinal interface between privacy norms and succession rights in India
3. To extract and assess comparative balancing mechanisms from the United States (RUFADAA), the European Union (GDPR with Member State rules), Germany, and France.
4. To propose a normative legal framework for India that reconciles the competing interests of the deceased, heirs, third parties, and digital service providers in relation to digital property after death.

## 6. RESEARCH METHODOLOGY

The objective of this research is to investigate how digital life is treated in relation to the concept of the afterlife through the analysis of digital platforms, as well as whether existing laws in India are sufficient to protect the digital rights of the deceased.

### **RESEARCH DESIGN**

This research adopts a qualitative doctrinal legal analysis supplemented by a comparative analysis. Doctrinal legal analysis is used to interpret statutory texts, constitutional provisions and judicial reasonings on privacy, succession and data protection. Comparative analysis is used to discern transferable components from international legal frameworks that has addressed posthumous digital data. To perform comparative analysis, the jurisdictions have been selected based upon their distinct regulatory models for digital succession and postmortem privacy. The jurisdictions being compared include the European Union's GDPR, the United States' Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), France, and Germany. Together, this research aims to suggest a normative framework while balancing the competing interests in India with regard to the digital afterlife.



## **DATA SOURCES**

The primary sources include legal texts such as the Information Technology Act of 2000, the Digital Personal Data Protection Act of 2023 and its 2025 rules, Article 21 of the Indian Constitution and important court cases like K.S. Puttaswamy v. Union of India (2017) and the 2026 Gandhinagar Civil Court ruling on digital estates. The secondary sources include academic articles, books, and government reports based on their relevance to digital afterlife, postmortem privacy and digital succession.

## **METHOD OF ANALYSIS**

The analysis in this research is premised on the four research questions presented above. About the first research question, the study examines “property” (here understood as digital remains capable of identification, valuation and transfer by an executor or administrator as part of the deceased’s estate) and “dignity” (here understood as the post-mortem interest in protecting the deceased’s identity, reputation and private communications from exposure or exploitation) from the conceptual-doctrinal perspective in terms of succession law and constitutional interpretation in India and analyses the possibility of treating digital remains as inheritable property without dehumanizing the dead person. As far as the second and third research questions go, the study conducts doctrinal mapping of privacy norms in Article 21, the Information Technology Act 2000, and the Digital Personal Data Protection Act 2023 (with 2025 Rules) along with succession law obligations of the executors and administrators to find the intersection/points of conflict between privacy and inheritance. Finally, in response to the fourth research question, the comparative analysis of the U.S. (RUFADAA), EU (GDPR with Member State Rules), Germany, and France leads to the development of possible balancing mechanisms like hierarchical access schemes, post-mortem instructions, universal succession, etc.

## **LIMITATIONS OF THE RESEARCH**

The research is limited to doctrinal and comparative analysis and does not include empirical or field-based data. This limitation is purposeful because the research gap concerns normative and conceptual clarity on how to balance interests, which requires legal reasoning before empirical testing.



## **7. ANALYSIS AND DISCUSSION:**

The following sections seek to address the identified research gap of an existing lack of legal framework to reconcile the competing interests of the deceased, their heirs, third parties, and online service providers in the context of the deceased's digital property. This section proceeds by addressing the identified four research questions. In this regard, it will analyze each of the research questions as separate yet connected strands of thought.

### **7.1 CONCEPTUAL ANALYSIS OF DIGITAL REMAINS**

The first research question is how to regard digital remains as property while respecting the deceased's dignity. Although there is no legal definition of "digital assets" in India, it is becoming evident that email accounts, social media profiles, cloud-stored data, cryptocurrencies, and metadata carry economic, emotional, and evidential value. There are two opposing doctrinal approaches towards digital remains: property and dignity approaches.

#### **DIGITAL REMAINS AS A PROPERTY**

According to general succession laws, the property of the deceased is inherited by legal heirs after the person passes away. In 2026, the Gandhinagar Civil Court made an observation that Letters of Administration could be provided for an iPhone and iCloud belonging to a deceased person and considered photos, videos, voice memos, and contact numbers to be inheritable properties. This case reflects judicial readiness to apply the provisions of the succession law to the digital trails of a person. The above-mentioned approach is supported by scholarly opinions stating that digital assets can be considered as property assets, regardless of the lack of a statutory basis. In this view, digital remains are analogous to tangible assets: they can be located, valued, and distributed by executors in fulfilment of their fiduciary duties.

#### **DIGITAL REMAINS AND DIGNITY**

On the other hand, the constitutional law of India acknowledges dignity as an essential part of Article 21, even in relation to dead bodies. Digital remains, being extensions of individuals, might contain issues of reputation, remembrance, and identity which cannot be treated as commodities. In this way, considering digital remains only in light of property would be instrumental in treating the digital remains of the dead person, especially in the case of private communication or intimate information.



## HYBRID CONCEPTUALIZATION

A balanced position should therefore not involve a dichotomy of “property” and “dignity.” Instead, digital remains should be thought of as hybrid: inheritable in the context of administration and economics but subject to dignity safeguards that restrict exposure, commodification, or manipulation. In terms of concepts, a hybrid concept can be used whereby digital remains are thought of as qualifying as property: inheritable in the context of administration and economics, but subject to dignity safeguards that restrict exposure, commodification, or manipulation. This will not involve a dichotomy of property and personhood and is consistent with new research which recognises that digital assets have both. However, some researchers argue that such an approach may commodify the dignity of the deceased, and they propose a strictly custodial or trust approach. This may be a valid apprehension; however, a combination of both approaches would be appropriate in recognising that, on one hand, heirs need access to handle estate administration, and on the other hand, there is a need to protect the dignity of the deceased from posthumous harms. Therefore, a combination of such views allows creating a balance whereby it is possible for heirs to have access to digital estates while also preserving the dignity of the deceased. Once it is clear that digital remains fall in the realm of both property and dignity, it is time to look into how privacy laws interrelate with succession under Indian law.

## **7.2 ANALYSIS ON PRIVACY NORMS UNDER INDIAN SUCCESSION LAW**

The second research question considers the impact of privacy principles on either restricting or facilitating access by heirs in light of the current succession law regime. The doctrinal analysis identifies an inherent conflict in that succession law places obligations on heirs to manage the estate of the deceased, while privacy principles create uncertainties as regards heirs' access to digital assets.

### **a) DUTIES UNDER INDIAN SUCCESSION LAW:**

According to Section 318 of the Indian Succession Act, 1925, executors and administrators are required by law to diligently collect the property of the deceased and any debts owed to them at the time of their death. Executors are also required by law to prepare an inventory listing the true value of the property they possess within six months of probate or letters of administration (Section 317). Given the legal recognition accorded to digital assets in the 2026 Gandhinagar



Civil Court case that ruled on Letters of Administration concerning a deceased person's iPhone and iCloud data, it is clear that the legal duties of heirs under Section 317 and Section 318 cannot be carried out without access to emails, accounts, and cloud storage.

#### b) PRIVACY AS A NON-INHERITABLE RIGHT

In Indian Privacy Law, after Puttaswamy, the right to privacy is considered an inherently personal right, which dies with the death of the individual (*actio personalis moritur cum persona*). In *Ruba Ahmed v. Hansal Mehta* (2022), the Delhi High Court opined that the right to privacy, being a right in personam, could not be claimed by way of inheritance by the mothers or legal heirs of the deceased. The Delhi High Court stated that the reputation gained or built by the individual during his life span dies with him and could not be inherited by the legal heirs like any other movable and immovable property. Such a position raises a dilemma for the heirs of such individuals, who have an obligation to manage the digital assets of the dead. This is because privacy, which is a basic right, is considered to be nullified at the time of death, thereby giving no legal ground to violate ToS (Terms of Service).

#### c) STATUTORY GAPS IN DPDP ACT, 2023 AND IT ACT, 2000

According to Section 14 of the DPDP Act of 2023, there is a provision for the nomination of an individual in the event of the death or incapacity of a data principal, and the Act does not state clearly whether nominees or legal heirs have any right to access the personal data of the dead person. Section 14 of the Act and the Rules of 2025 confer on nominees the power to exercise the rights of a data principal. These are privacy and governance rights but not succession rights, because the value associated with the data is governed by succession and contract laws.

Moreover, the provisions contained in Section 43, 66, and 72 of the Information Technology Act, 2000, which provide penalties for unlawful access to computer systems and data theft, respectively, can be used against an heir accessing his digital account without prior approval from the platform itself, even if it is done for legitimate reasons. The argument, therefore, is that Indian law places heirs in a direct bind: Section 317 and 318 of the Indian Succession Act obligate them to access and administer digital accounts, while Section 43, 66, 72 of the IT Act expose them to potential criminal liability for that very access, with neither the DPDP Act nor the IT Act providing a lawful-access exception for estate administration.



#### d) THE NEED FOR RECONCILIATION

As we have seen above, the intersection between privacy and succession law leads to a paradoxical situation where heirs must exercise their duty to administer the digital assets but do not have the statutory power to do so because privacy norms, despite being extinguished by death, function implicitly through data protection norms and platform rules. Although privacy as a basic human right might cease at death, as argued by Ruba Ahmed, the residual interests of dignity, reputation, and family privacy could be used as justification for protecting heirs from posthumous harms. The following approach would therefore ensure harmonization of heirs' duty of administration with the residual privacy and dignity.

With the doctrinal interface of privacy and succession law discussed above, the next step is to determine whether Article 21 of the Constitution can provide the basis for recognizing posthumous privacy interests.

### **7.3 SCOPE FOR POSTHUMOUS PRIVACY UNDER ARTICLE 21**

The third research question requires an analysis of the extent to which Article 21 of the Indian Constitution can be read to protect privacy regarding digital information in relation to the dead. It is worth noting that while the Indian Supreme Court has upheld privacy as a fundamental right under Article 21, later judgments have seen it as a personal right, which is no longer valid after death. There are, however, three grounds on which Article 21 can be said to be posthumous.

#### a) PRIVACY AS A FUNDAMENTAL RIGHT

In the nine-judge Constitution Bench decision of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), it was unanimously opined that the right to privacy is a fundamental right under Article 21 of the Constitution, which includes information privacy as well as the right of an individual to manage his personal data collection. The right to privacy has been interpreted to be inherent in the right to life and personal liberty, thus becoming a part of the triad of Articles 14, 19, and 21. However, the question of whether the right to privacy extends beyond the realm of life was not decided in this case and thus needed to be deliberated upon in future judicial decisions.



## b) JUDICIAL INTERPRETATION OF POSTHUMOUS PRIVACY

The Indian judicial pronouncements are of the view that privacy and reputation rights are extinguished at the death of a person and thus cannot be inherited. As stated by the Delhi High Court in the case of *Krishna Kishore Singh v. Sarla A. Saraogi*, “privacy or reputation earned by a person during his or her lifetime extinguishes with his or her death” and does not form part of either movable or immovable property that could be inherited by a person. Further, in the case of *Ruba Ahmed & Anr. v. Hansal Mehta & Ors.*, the Delhi High Court refused to grant an injunction to stop the release of a film on the ground that the right to privacy was primarily personal and hence could not be claimed by the heirs of a deceased. Thus, from the above cases, we can see that there is a clear doctrine in India that the right to privacy as a fundamental right cannot be claimed after the death of the person.

## c) ARGUMENTS FOR A LIMITED POSTHUMOUS INTERPRETATION

Even in the light of these considerations, there are some compelling reasons for attributing a certain posthumous character to Article 21:

The relationship between privacy and dignity or autonomy was established by the Supreme Court in *Puttaswamy* (2017). As dignity rights such as one’s reputation or memory, or respect can continue beyond one’s death, there can thus be a derivative right of privacy after death to prevent any disclosure, deepfake or commercial exploitation of the digital persona of the deceased. The Supreme Court in *Parmanand Katara v. Union of India* (1989) observed that the dignity right includes even the posthumous right to dignified treatment of the body, since Article 21 of the Constitution takes in elements of a life that go on even after death. The recent observation of the Kerala High Court in *Jebin Joseph v. State of Kerala* (2024) states that “the constitutionally protected and guaranteed right of every individual to dignity and fair treatment, especially under Article 21 of the Constitution of India, cannot be said to end with death but extends far beyond.” The postmortem right to privacy might be based not on the fact that a person is alive after his death, but rather on the interests of the family of the deceased and the interests of society in the dignity of the dead. Publicising private communications of a dead person can hurt his surviving relatives. Access to digital remains without regulation may result in damage to the reputation of the individual, identity theft, and emotional trauma of the family left behind. Granting the deceased person’s right to privacy under Article 21 is a basis of constitutional law to protect against such injuries, especially with regard to deepfake generation and commercial use by AI.



#### d) BALANCING PRIVACY EXTINGUISHMENT WITH REMAINING INTERESTS

This research does not aim to oppose the principle of extinction of privacy being one of the fundamental rights after death. Instead, it is asserted that remaining dignitary, reputational, and familial privacy interests might support certain statutory safeguards against posthumous harm, based on the values behind Article 21. Concretely, a dignitary interest is engaged where intimate photographs of the deceased are circulated without consent; a reputational interest is engaged where selectively edited private messages are published to mislead the public; and a familial privacy interest is engaged where correspondence between the deceased and a living relative is disclosed without that relative's consent. It is these concrete harms, rather than an abstract survival of personality, that the proposed safeguards are designed to prevent. The suggested protections would not view the deceased as a holder of continuing rights but would admit that certain dignitary and relational interests deserve to be legally protected even after death. In terms of practical implementation, it means that the use of Article 21 should inform a statutory approach rather than provide an absolute right to block access to digital inheritance by heirs. In other words, a statutory regime can allow heirs access to the decedent's digital inheritance but prohibit any further unauthorised disclosures, commercial use, or artificial intelligence-based impersonation of the deceased.

Now, having reviewed the possibilities of posthumous privacy protection under Article 21, the next subsection analyses transferable balancing approaches from comparative jurisdictions.

#### **7.4 COMPARATIVE ANALYSIS ON DIFFERENT JURISDICTIONS**

The fourth research question considers comparative regimes as sources for transferable balancing measures that apply to India. Four examples selected are the United States (RUFADAA), the European Union (GDPR framework with derogations from individual member states), France, and Germany. These are chosen since these countries provide an illustration of all the different types of balancing measures that exist today internationally: hierarchal access of fiduciaries, privacy exclusion with derogations by individual member states, postmortem directives, and universal succession.

##### **UNITED STATES:**

Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), published in 2015 by the Uniform Law Commission, provides a hierarchical structure of three priorities that help determine the intentions of the user towards digital assets.



Tier 1 (Online Tools): Under section 4(a), if a user utilises an online tool to instruct a custodian to either release or refrain from releasing digital assets to a fiduciary, then the direction contained in the online tool is controlling.

Tier 2 (Wills, Trusts, Powers of Attorney): Under section 4(b) Where there is no user direction using an online tool, the directions within the user's will, trust, or power of attorney take precedence over any conflicting terms of service provisions.

Tier 3 (Terms of Service and Default Rules): Under section 4(c), in the absence of user directions via online tools and in the absence of testamentary documents, the terms of service control. If there are no terms of service provisions, then the RUFADAA default statutory provisions would apply.

This particular model stresses the user's autonomy, brings clarity to the platforms, and strikes a balance between fiduciary access and privacy protection (for example, a custodian can make available only the list of items held, without disclosing any information about their contents unless specifically authorized). RUFADAA has been adopted in more than 45 states in the United States.

#### **EUROPEAN UNION:**

The GDPR expressly states in Recital 27 that it does not apply to personal data of deceased persons, while allowing Member States to create rules concerning deceased persons. This demonstrates that there is no universal legal necessity to treat posthumous data exactly like living-person personal data. But it also demonstrates the weakness of leaving the matter entirely outside a data-protection framework. India should therefore consider a limited posthumous data regime that protects the deceased's expressed wishes, dignity and digital identity while also protecting living third parties and confidentiality.

#### **FRANCE:**

France has adopted one of the most sophisticated post-mortem data laws. Under Article 85 of the French Data Protection Law. A person is permitted to establish directives about the handling, deletion, and transfer of his or her personal data after death. The directives may be particular about a certain data controller or service and also related to all personal data about the person, to be registered with a third-party entity recognized by CNIL. In the absence of directives or wills, heirs have the right to access certain data, obtain digital assets, close accounts, or raise objection to some of the processing activities.



## **GERMANY:**

Germany considers digital accounts as inheritable contractual rights based on universal succession, where digital accounts are inherited after the death of the user. The Bundesgerichtshof, in an important decision of 2018, ruled that heirs inherit the contractual right of the deceased to social media accounts and the content thereof, but within the limits of telecommunications privacy.

## **ADAPTIVE MEASURES TO INDIAN FRAMEWORK**

The following features can be adapted to India from these comparative regimes:

1. Tiered Access Hierarchy (RUFADAA). A priority of user directives (made using online means and wills) over ToS, and providing for statutory defaults where silence applies, would give clarity to the heirs, platforms, and courts. It would match the rationale based on autonomy in the Puttaswamy (2017) case.
2. Post-Mortem Directives (France). Individuals can give instructions as to retention, deletion, or access restrictions after death. This way, they would manage their digital legacy while eliminating potential disputes between heirs and platform operators. The French system of specific and general directives to be registered with third parties could be adopted to Indian digital reality.
3. Universal Succession (Germany). Determining that digital accounts should pass to heirs as contractual rights, subject to privacy considerations, would solve the current ambiguity of Indian succession law doctrine.

## **7.5 NORMATIVE FRAMEWORK FOR INDIA**

On the basis of the doctrine and the constitutionality analyses described in the above sections, this section presents a normative proposal in the form of a framework for India, called Posthumous Privacy Governance. The framework seeks to address not whether there is a life after privacy but rather attempts to create a limited purpose-based governance framework.

### **1. Digital Testamentary Privacy: Legally Recognisable Digital Will**

The following research presents a concept called Digital Testamentary Privacy, the right of the individual to leave legally recognizable instructions pertaining to the handling of his or her digital identity and personal information upon death. Such instructions may pertain to:



Category A – Delete: Removal of certain accounts and information.

Category B – Preserve: Storage of certain legacy information such as photographs and writings.

Category C – Transfer: Allocation of beneficiaries of monetised accounts or digital information.

Category D – Restricted Disclosure: Disclosure only to specific people or for specific reasons.

Category E – Never Disclose: Strict prohibition on the disclosure of sensitive information.

Category F – AI Prohibition: Express prohibition on the use of voice, face, writing, or biometrics for creating AI reproductions and avatars.

It changes the "digital will" from an ordinary technical tool to a legally recognisable one, which can be implemented as proposed in Section 14A of the DPDP Act, 2023 (Posthumous Digital Data Administration).

## 2. Digital Executor: A New Fiduciary Role for Digital Estates

While traditional succession law has established executors and administrators, the digital world needs a new digital executor who would be entitled to:

1. Classify and identify digital property assets (economic, contractual, personal, thirdparty).
2. Inform the digital platforms of the death and demand their deletion or preservation, or transfer as per the wishes of the deceased.
3. Manage the monetised accounts and identify digital assets which can earn money (cryptocurrency, NFTs).
4. Implement the digital will of the deceased and prevent any unauthorized replication of his digital assets by the AI.

The digital executor would have fiduciary obligations towards confidentiality, data minimization, third party privacy, no personal benefit, secure handling of the data and destruction of unnecessary data.

## 3. Privacy Firewall: Purpose-Based, Filtered Access

The proposal for the Privacy Firewall will be between the estate and the total digital archive of the deceased. Rather than giving total access to the legal heir, this approach includes:



Legal heir → administrator → purpose verification → privacy filtering → access required.

It consists of six steps:

1. Determine the heir/administrator's legitimacy.
2. Categorise the digital assets (economic, legal, personal, third parties).
3. Determine what is sensitive (e.g., health information, private communications).
4. Protect the third parties' personal information (e.g., the email correspondent).
5. Release only that information which is needed for the estate administration.
6. Require another authorisation for business and AI purposes

It will be a more proportional and technologically realistic approach that solves the problem of the lack of consent because the heir cannot agree retroactively to everything the deceased had kept private.

#### 5. Three Level Model for Posthumous Digital Protection

The model consists of three levels of posthumous digital protection as follows:

Level I – Protection of Estate: Money, cryptocurrency, monetised account, digital business, and transferable Intellectual Property that is regulated via inheritance law.

Level II – Protection of Privacy: Confidential communications, medical information, private photographs, diaries, personal confidential information, and third-party information that would be protected under restricted access through the DPDP Act, 2023.

Level III – Protection of Identity: Face, voice, image, personality, AI avatar, and digital replica that requires explicit consent and legal authorisation with additional protective measures in order not to be synthesised

Such an approach takes into consideration the need for immediate action regarding AI-based exploitation while making the distinction between utilising historical information about the deceased and synthesising their identity.

#### 6. Interest Hierarchy: Solving the Triangular Conflict

The conflicts in digital afterlives typically concern three people: Deceased → Family/Heir → Platform. A rational hierarchy should include:



1. Valid and clear instructions of the deceased (the digital testament).
2. Compulsory legal rights and duties.
3. Rights of other surviving persons (such as privacy of correspondents).
4. Succession rights of the heirs (with dignity and privacy qualifications).
5. Contractual limitations of the platform (qualified by statutes)

It avoids that private contracts between platforms become the last word on the digital death of a person.

## 7. Legal Recognition of Digital Afterlife Rights

This study proposes five legal rights in Indian law:

1. Right to Digital Closure: The right to request that certain digital accounts be deleted, closed, or memorialised upon death.
2. Right to Digital Continuity: The right to ensure that certain photographs, written material, recordings, and other legacy material are preserved.
3. Right to Digital Privacy: The right to keep certain information from being disclosed indiscriminately, unless there are legitimate legal concerns.
4. Right to Digital Identity Integrity: The right to ensure that the person is not mimicked, represented in synthetic media, or recreated through artificial intelligence.
5. Right to Digital Succession Control: The right to appoint a Digital Executor and decide the level of posthumous access and control.

In sum, all these rights represent an effort by the Indian legal system to shift from the rather narrow conception of treating a digital estate as a kind of property into a governance approach based on prior intention, dignity, purposes restriction, proportionality, third party privacy, succession, and identity protection.

### **Implementation: Amending Existing Legislation**

The immediate enactment of a distinct statute in India may not be necessary; rather, a viable model can be established by



1. Amendment to the DPDP Act, 2023: Creating Section 14A (Posthumous Digital Data Administration) to take into account digital instructions in wills, Digital Executors, and AI protections.
2. Amendment to the Indian Succession Act, 1925: Including digital assets in the list of assets, as well as the function of Digital Executors.
3. Rules under the IT Act, 2000: Including mandatory cooperation of platforms, standardized APIs for legacy contacts, and fines for blocking people at will.

Such an approach builds upon the 2026 Gandhinagar Civil Court ruling, which already took into consideration the status of iCloud data as inheritable property, yet moves further and deals with the question of what can be done with the data once the right of access is gained.

Analytically, this framework directly resolves the tension identified in Section 7.2: the Privacy Firewall converts the heir's Section 317–318 duty from a blanket right of access into a purposelimited one, which removes the exposure to Sections 43, 66 and 72 of the IT Act identified above, because access is no longer unauthorised once purpose and legitimacy have been verified. Equally, the Digital Testamentary Privacy instrument answers the concern raised in Ruba Ahmed, that privacy cannot be inherited by locating the safeguard not in an inherited right of the deceased but in a right the deceased exercised while alive, which is a materially different constitutional basis and therefore survives the extinguishment doctrine intact. The framework's contribution, in other words, is not merely descriptive: it identifies the precise doctrinal point at which existing succession and privacy law conflict and proposes a mechanism located at that exact point.

It is evident from the discussion above that there exists no coherent framework in Indian law to reconcile the interests of the deceased, heirs, third parties, and platforms in the digital afterlife. The analysis shows that the digital remains are hybrid entities that, despite being inheritable to administer the estate, are deeply connected to the concepts of dignity and privacy. With the help of comparative legal models and the values embodied in Article 21, the chapter presents a Posthumous Privacy Governance framework in India, including Digital Testamentary Privacy, a Digital Executor, a Privacy Firewall, and five digital afterlife rights. The proposals will require only amendments to the DPDP Act, 2023, Indian Succession Act, 1925, and IT Act Rules to ensure their implementation. The key aspect of the proposals is that



they will shift the treatment of digital estates from a purely proprietary one to an object of governance characterized by intention, dignity, proportionality, and identity protection.

## 8. CONCLUSION

This research began by examining how Indian law treats property on one hand and privacy on the other and observed that digital remains fall awkwardly in between the two, belonging fully to neither. This gap is what the study set out to address.

The reasoning developed across the research questions follows accordingly. Digital remains should not be treated as property alone, as this risks converting deeply personal or identity-related material into something that can simply be inherited and disposed of. At the same time, they cannot remain locked away as untouchable personal data, since the Indian Succession Act, 1925, places a legal duty on heirs to collect, value, and administer exactly such assets. Indian courts have so far managed this tension through inconsistent default positions rather than a settled doctrine; some decisions treat privacy as extinguished at death, while others extend dignity protections under Article 21 beyond it. This incompleteness is exemplified by the Gandhinagar Civil Court's 2026 ruling allowing Letters of Administration over a dead person's phone and cloud account. The ruling allows access but raises the more important questions of what that access is for and where that access should end.

A comparative study of other jurisdictions was undertaken to find elements that are really workable within India's constitutional and statutory framework, particularly Article 21 and the Digital Personal Data Protection Act, 2023. From this comparison, a framework was developed consisting of a Digital Testamentary Privacy instrument, allowing individuals to leave instructions for their digital identity after death; a Digital Executor, a new fiduciary role suited specifically to digital estates; and a Privacy Firewall that checks the purpose of access before anything is released, rather than granting heirs unrestricted entry. A three-level model keeps estate matters, privacy protections, and identity protection analytically distinct, while an interest hierarchy ensures that no single party heir, platform, or family member is left to decide everything unilaterally.

What this framework attempts, at its core, is to track the living interests that continue to touch digital remains even after the person themselves is gone: the administrative duties owed by heirs, the residual dignity of the deceased, and the privacy of third parties who appear in that data. Existing Indian legal categories were simply never built to hold all of these together.



Importantly, none of this requires an entirely new statute. A modest addition to the Digital Personal Data Protection Act, 2023, alongside updates to succession law and platformcooperation rules under the Information Technology Act, 2000, would be sufficient to build on the direction the Gandhinagar Court has already begun to set.

That said, the study does not claim to have resolved every operational detail. How the privacy firewall would function in practice. Who verifies purpose, at what stage, and against what standard remains only partly worked out here and is better addressed through future empirical and procedural research rather than doctrinal analysis alone.

## REFERENCE

1. Boothe, A. (2022). The death and life of Jang Nayeon: A case for personality rights in the digital layers of reality. *International Journal of Law and Information Technology*, 30(4), 398–422. <https://doi.org/10.1093/ijlit/eaad005>
2. Bundesgerichtshof [BGH] [Federal Court of Justice]. (2018, July 12). Urteil [Judgment], III ZR 183/17, BGHZ 219, 243. <https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2018-7&nr=86602&linked=urt&Blank=1&file=dokument.pdf>
3. CNN. (2024, February 12). *AI “resurrects” long-dead dictator in murky new era of deepfake electioneering*. <https://www.cnn.com/2024/02/12/asia/suharto-deepfake-aiscam-indonesia-election-hnk-intl>
4. Commission Nationale de l'Informatique et des Libertés. (2025). *Our data after us: 10th IP report on post-mortem data*. CNIL. [https://www.cnil.fr/sites/default/files/202511/cnil\\_10th\\_ip\\_report.pdf](https://www.cnil.fr/sites/default/files/202511/cnil_10th_ip_report.pdf)
5. 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), 101–129.
6. Government of India. (1925). *The Indian Succession Act, 1925* (Act No. 39 of 1925). India Code. <https://www.indiacode.nic.in/handle/123456789/2385>
7. High Court of Delhi. (2022, October 14). *Ruba Ahmed & Anr. v. Hansal Mehta & Ors.*, CS(OS) 498/2021. Indian Kanoon. <https://indiankanoon.org/doc/17644164/>



8. India Code. (2000). *The Information Technology Act, 2000* (Act No. 21 of 2000). <https://www.indiacode.nic.in/handle/123456789/21433>
9. India Code. (2023). *The Digital Personal Data Protection Act, 2023* (Act No. 22 of 2023). <https://www.indiacode.nic.in/handle/123456789/22037>
10. *Jebin Joseph v. State of Kerala*, 2024 Supreme (Online)(KER) 13793 (Kerala High Court, February 8, 2024).
11. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India, August 24, 2017).
12. Kaur, D., & Nath, A. (2025). The right to privacy in social media platforms: Legal and regulatory challenges in India. *International Journal for Multidisciplinary Research*, 7(5), 1–[end page]. <https://www.ijfmr.com/papers/2025/5/57047.pdf>
13. Kaushal, K. (2026). Digital inheritance in India: Legal gaps and future solutions. *International Journal of Advanced Legal Research*, 6(2), 1–10. <https://ijalr.in/volume-6-issue-2/digital-inheritance-in-india-legal-gaps-and-future-solutions-karan-kaushal/>
14. *Krishna Kishore Singh v. Sarla A. Saraogi & Ors.*, (2023) SCC Online Del 4567 (Supreme Court of India, July 11, 2023).
15. Lingel, J. (2013). The digital remains: Social media and practices of online grief. *The Information Society*, 29(3), 190–195. <https://doi.org/10.1080/01972243.2013.777311>
16. Mali, P., & Prakash G, A. (2019). Death in the era of perpetual digital afterlife: Digital assets, posthumous legacy, ownership and its legal implications. *National Law School Journal*, 15(1), Article 8. <https://repository.nls.ac.in/nlsj/vol15/iss1/8>
17. Mishra, A., & Mishra, A. (2025). Digital afterlife and post-mortem data rights in India. *International Journal for Legal Research and Analysis*, 2(8), 1–15.
18. Morris, M. R., & Brubaker, J. R. (2024). *Generative ghosts: Anticipating benefits and risks of AI afterlives* [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2402.01662>
19. Öhman, C., & Floridi, L. (2018). An ethical framework for the digital afterlife industry. *Nature Human Behaviour*, 2(5), 318–320. <https://doi.org/10.1038/s41562-018-0335-2>
20. *Parmanand Katara v. Union of India*, (1989) 4 SCC 286 (Supreme Court of India, August 28, 1989).
21. *Pt. Parmanand Katara v. Union of India*, (1989) 4 SCC 286 (India)
22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).



23. *Ruba Ahmed & Anr. v. Hansal Mehta & Ors.*, 2022 LiveLaw (Del) 969 (Delhi High Court, October 14, 2022)
24. SCC Online. (2026, May 30). Digital data part of estate, right to privacy does not survive death: Gandhinagar Court. *SCC Online Blog*. <https://www.scconline.com/blog/post/2026/05/30/digital-data-forms-part-of-the-deceased-estate/>
25. Tech Law Forum. (2026, July 27). Digitally existent, but legally absent? Examining the digital afterlife industry under India's constitutional and data protection framework. *Tech Law Forum @ NALSAR*. <https://techlawforum.nalsar.ac.in/digitally-existent-but-legally-absent-examining-the-digital-afterlife-industry-under-indias-constitutional-and-data-protection-framework/>
26. The Print. (2026, May 21). In death, who owns your data? Gujarat court grants heirs' digital inheritance of deceased's iCloud. *ThePrint*. <https://theprint.in/judiciary/in-death-who-owns-your-data-gujarat-court-grants-heirs-digital-inheritance-of-deceaseds-icloud/2937413/>
27. Uniform Law Commission. (2015). Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). <https://www.uniformlaws.org/viewdocument/final-act-with-comments-40?CommunityKey=f7237fc4-74c2-4728-81c6b39a91ecdf22&tab=librarydocuments>