

---

## DIGNITY BEYOND DEATH: LAW, AI, AND THE FORGOTTEN RIGHT TO DIGITAL REST

---

Pragati Mishra, Lawyer

### ABSTRACT

The digital advancement has altered the meaning of death. The digital life continues to exist even after biological life of an individual via cloud storage, social media accounts, biometric databases, and AI systems that can imitate voice, behaviour, and personality. Where, for the law the protection extending to privacy, autonomy, dignity ends with biological life, the digital life continues to exist without any legal protection or oversight thereby creating a legal vacuum. This paper conceptualises such posthumous data as “digital orphan” i.e. the digital remains without a legal guardian, vulnerable to cybercrime, data manipulation, commercial and emotional exploitation. The deceased and even their families continue to remain victims of crimes without any legal authority to protect them. The study analyses the current legal system including the constitution, data protection law, cybercrime statutes, and succession law and demonstrates how the existing legal framework is incompetent to deal with the posthumous data rights. Constitutional interpretation of dignity and privacy as personal rights combined with the absence of any legal and regulatory framework to protect the rights, the posthumous data is left largely at the hand of the private platforms governed by contractual obligations which are made for commercial gains. The paper further compares the legal developments in the jurisdictions of China, Estonia, Germany, and the US to inspect the emerging fiduciary digital access and posthumous data regulation. It ultimately suggests how a shift in the legal, regulatory, policy and governance by treating this posthumous data as an abandoned information to an extension of human dignity and human right value can advance the concept of “right to digital rest” as an essential principle in the technological advancement.

**Key Words:** - *Digital orphans, Posthumous Data, Techno-legal gap, Cybercrimes, Data Privacy, Dignity.*

## I. INTRODUCTION

The concept of death has changed in digital age. Even after a person's cremation or burial, digital footprints such as photos, videos, voice notes, internet activities are still stored in the cloud servers and can be searched. Their phones continue to receive bank alerts, OTPs, social media accounts remind the family members of their birthdays and other occasions. These memories can not only be strange, painful, and heartbreaking but also the continued digital presence is dangerous and confusing from a legal standpoint<sup>1</sup>

The Netflix series mismatched reflects the issues linked to the digital age when an AI based chatbot was created which mimicked lead's father's voice, though emotional and having a touching tribute, questions such as identity misappropriation, emotional manipulation, unaddressed consent frameworks, posthumous data usage were brought forth which are yet not sufficiently addressed by legal framework. An emotional AI usage for recreating or preserving digital data of loved ones not merely poses serious legal and ethical risks but also highlights that digital death is not possible in current scenarios. What rights should individuals and family members have to prevent the digital data outlive our self? What regulatory and legal frameworks must be adopted to not only preserve our digital self being compromised during our life but also in after-life? Current law treats the right to privacy as being born and end with an individual's life thereby stopping to legally recognise the data and its vulnerabilities after death<sup>2</sup>. This situation creates "digital orphans" where personal data is present without any legal guardian, such data is more prone to frauds, identity thefts, impersonation, cybercrimes. The article tries to examine the legal gap between technological advancement and legal shortcomings thereby addressing a way to fill the gap to protect and prevent our digital self from being compromised after our life.

## II. DIGITAL ORPHANS: ABANDONED DATA AS A NEW VICTIM TO CRIME

The digital India mission transformed the country into a globally leading digital economy due to which a person leaves not only physical belongings but also vast digital information including social media accounts, emails, cloud stored photographs, online banking, UPI transactions, voice

---

<sup>1</sup> Nishchay Rao, *Data after death: legal consequences of posthumous data management* (2024) 2 Braz J Law Tech & Innov 71

<sup>2</sup> Michael Birnhack and Tal Morse, 'Digital Remains: Property or Privacy?' (2022) 30(3) *International Journal of Law and Information Technology* 280–307.

notes, e-commerce histories, education and health profiles, government platforms such as Digi Locker. These are generally referred as digital footprint<sup>3</sup>.

A person's online presence does not simply disappear after they pass away. Data and accounts belonging to an individual are frequently stored on servers for years or even permanently. The family members do not automatically have access to, control over, or legal power over this information. Rather, it is held by the government and private businesses. Unattended personal data is referred to as "digital orphans" because it has outlived its owners and no one has an effective legal authority over it. Unlike physical property, which is passed down through inheritance, personal data is kept hidden behind privacy policies, regulatory barriers, and rules<sup>4</sup>.

The risks associated with personal data are significant and long-lasting. Once the data is compromised, families may experience emotional distress, financial loss, and reputational risk. Email accounts can be compromised, documents can be used for identity theft, images and voice recordings can be used to train AI or create deepfakes that sound and look authentic, and even a discarded SIM card can provide someone else access to private messages and data. The digital remains are no longer harmless recollections but are active targets for exploitation.

Digital illiteracy and unawareness are a major contributing factor to the issue. Most people are unaware that, like with tangible possessions, managing your digital life involves forethought. In India, the idea of digital wills is still missing<sup>5</sup>. Without them, families face a lot of legal and technical obstacles and serious security risks

### **III. AFTER DEATH BEFORE LAW: GAPS IN INDIAN LAWS ON DIGITAL IDENTITY AFTER LIFE**

When it comes to digital data protection, India does have some laws however they are not expansive enough to cover the data after death. Below is an in-depth analysis of key legal provisions, what they cover and how they fall short for “digital orphans”

---

<sup>3</sup> Edina Harbinja, *Digital Death, Digital Assets and Post-mortem Privacy: Theory, Technology and the Law* (Edinburgh University Press, Edinburgh, 2022).

<sup>4</sup> Janneke Gerards, Sanne Kruijemeier and Eleni Kosta, ‘Post-mortem Privacy and Informational Self-Determination’ (2017) 19(2) *Ethics and Information Technology* 129–142.

<sup>5</sup> Birnhack and Morse, *supra* note 1.

### **A. Digital Personal Data Protection Act, 2023 (DPDP Act)<sup>6</sup>**

India's first comprehensive law on data privacy, protection and giving rights to individual whose data is being processed. Section 6 deals with clear consent and section 11 with certain important rights of individuals such as right to nominate and right to erasure.

Though the law recognises nomination rights, the act does not mandate nomination. If an individual dies without appointing a nominee, their personal data is left under the control of private companies. Further it is silent on the rights of heirs if there is no nominee. It does not treat data as inheritable property under succession laws.

Therefore, if the "data principal" dies the protections under the Act become theoretically exercisable only through a nominated representative- hence leaving a void if none was appointed.

### **B. Information Technology Act,2000<sup>7</sup>**

The IT Act is primary cybercrime statute and defines offences involving computers and digital systems. The act does not automatically provide privacy rights rather it criminalises misuse of digital systems including identity theft and impersonation and breach of privacy

The act's primary protection provisions such as section 43A (compensation for failure to protect data) and 72A (punishment for disclosure in breach of contract) focuses on living "data principals".

Some provisions such as section 66 i.e. identity theft, 66D i.e. cheating by personation using computer resource and 72 i.e. breach of privacy can apply to posthumous misuse but they are reactive i.e. apply only when the crime has occurred. They fail to create proactive rights for families to control or delete a deceased's person's digital data

Section 1(4) excludes its application to wills and other testamentary dispositions. Therefore, the provision of "digital will" is absent from the act.

---

<sup>6</sup> The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

<sup>7</sup> The Information Technology Act, 2000 (Act No. 21 of 2000).

The act does not recognise “digital data” as inheritable property hence the privacy linked to these records are non-transferable under the Act

Technically, an heir who accesses deceased person’s accounts- even with good intentions- would be punished under section 43 and 66 of the Act due to unauthorised access to computer systems.

### **C. Bhartiya Nyaya Sanhita,2023<sup>8</sup>**

Section 318 i.e. cheating and dishonest inducement.The provision helps prosecute frauds but is silent on the question of handling the data after the death of the person

Section 356 i.e. defamation sets a high bar for the crime and focusses more on survivor’s feeling upon reputational harm of the deceased rather than deceased’s inherent data privacy.

It is difficult to punish crime against digital data and accounts as offences against movable property such as theft or criminal misappropriation and the digital data has not yet been classified as a movable property by the courts.

### **D. Indian Succession Act,1925<sup>9</sup>**

Section 2(a) of ISA has not been updated to include digital assets such as an email, cloud storage, accounts etc as movable property

Digital wills are not formally recognised under the ISA.

Digital accounts are still governed by service provider agreements rather than inheritance laws

No statutory authority such as “digital executor” without which the heirs who attempt to use digital data of deceased person are liable under IT Act.

No clear guidelines are provided in succession laws as to who inherits a monetized YouTube channel or a domain name or a cryptocurrency wallet.

### **E. Jurisprudence and Posthumous rights**

---

<sup>8</sup> The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).

<sup>9</sup> The Indian Succession Act, 1925 (Act No. 39 of 1925).

Landmark Supreme court ruling in *Justice KS Puttaswamy(retd) vs Union of India 2017*<sup>10</sup> established privacy as a fundamental right emanating directly from Article 14,19 and 21 of the constitution and held privacy, dignity, autonomy, and personal liberty as inviolable principles of law. The case helps argue that data protection and dignity are rooted in the constitutional values. The court held that the right to privacy is born with the individuals and extinguishes with them. Justice Abhay Manohar Sapre explicitly stated that the right remains with an individual only “till he breathes his last.”

The judiciary relies on the maxim of *actio personalis moritur cum persona* i.e. a personal right of a person dies with the person. This prevents the heir from suing for privacy violations such as unauthorised disclosure of transaction history or private mails.

The judgement recognised the right to be forgotten however, after the person has deceased and no other clear law allows the heir to exercise the right it becomes quite impossible to have the sensitive data of the deceased erased from the internet.

Delhi High Court judgment in *Krishna Kishore Singh vs Sarla A. Saraogi &Ors 2022*<sup>11</sup> the court held that the right to privacy, publicity and personality rights do not survive death and cannot be inherited by a legal heir. Further, in *Ruba Ahmed &Ors vs Hansal Mehta & Ors*<sup>12</sup>the Delhi High Court held that privacy rights are in personam and therefore not inheritable by legal heirs once a person dies.

The legal implications of the above judgments clearly shows that while the constitution strongly protects personal data during a person’s lifetime, the moment death occurs, the legal shield collapses. A serious gap between constitutional theory and technological reality is brought to light.

#### **IV. DIGITAL DIGNITY AND A CONTINUED SOURCE OF CONSTITUTIONAL AND HUMAN RIGHTS VALUE IN THE AGE AI**

AI has disrupted the traditional legal presumption that dignity rights are born and die with the person’s biological death. Digital technologies have been able to continue the functional

---

<sup>10</sup> Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.

<sup>11</sup> Krishna Kishore Singh v Sarla A. Saraogi & Ors, 2022 SCC OnLine Del 1229.

<sup>12</sup> Ruba Ahmed & Ors v Hansal Mehta & Ors, 2022 SCC OnLine Del 403.

existence of human through continuous data storage, algorithmic profiling, AI generated simulations. Even after physical death, individuals' identity continues to be operated in the digital space when his voice recordings, facial images, behavioural data is used for machine learning. This phenomenon known as "functional survival" of digital personality bypasses the traditional constitutional protections<sup>13</sup>.

Recent proactive approaches have shown that the constitutional law has recognised the post bodily life dignity when it extends dignity to respectful handling of human corpse, burial rights<sup>14</sup>, and protection of reputation. In the digital era, AI can actively transform data into artificial representations, clone voice, chatbots, predictive personality models, these substitutes can think, function and speak to others using the data of the deceased therefore, the personal data can create relational, reputational, emotional harms to an individual hence and unregulated usage of data post biological life can cause as much exploitation as can be caused in biological life. The absence of active consent mechanism converts the individuals into a source of training for emotional and commercial based AI applications. This undermines autonomy and exposes families to several risks.

Instruments such as UDHR<sup>15</sup>, ICCPR<sup>16</sup> have long recognised dignity as a foundation to the interpretation to other basic human rights such as privacy, reputation, and protection from degrading treatment. The human rights framework imposes a positive obligation upon the states to protect the individuals by regulating the private players when the technological system poses a foreseeable risk to the fundamental values<sup>17</sup>. Most of the formal human rights treaties have actively protected the living human, human rights jurisprudence acknowledges the protection should extend beyond when interests are connected to identity, memory, and reputation, especially in cases when any violations to these can affect the surviving family members or the society at large. The misuse of data can affect both the deceased individual and the family hence leaving the data protection to contractual terms of the corporations without state oversight conflicts with the state's duty to protect the dignity against non-state actors. Hence, from human rights jurisprudence, posthumous data protection laws are not

---

<sup>13</sup> Edina Harbinja, *Digital Death, Digital Assets and Post-mortem Privacy* (Edinburgh University Press 2022) ch 5.

<sup>14</sup> *Ashray Adhikar Abhiyan v Union of India*, (2002) 2 SCC 27.

<sup>15</sup> Universal Declaration of Human Rights, GA Res 217A (III), UN Doc A/810 (1948), arts 1, 12.

<sup>16</sup> International Covenant on Civil and Political Rights, 1966, 999 UNTS 171, arts 7, 17.

<sup>17</sup> *Vishaka v State of Rajasthan*, (1997) 6 SCC 241.

merely an issue of succession or contractual obligations but the obligation to preserve the human dignity in the digital age to prevent the technological advancement bypassing universality of dignity.

## V. FROM PUTTASWAMY TO PLATFORM POLICIES

In the absence of legal regulation on the topic, private companies have undertaken the responsibility. Offers like memorialized accounts, legacy contacts or inactive account managers are being offered by social media platforms and email service providers. These are not legal rights rather are completely based upon the company policies however, they seem to provide some solution to the handling of data after death but, these are not sufficient

Firstly, these policies are completely dependent on whether the user activated them while they were still alive. Most Indians lack digital literacy. Families might have to undergo complex system of requirements<sup>18</sup>, submit death certificates, require customer support and still be unsure of whether access or deletion will be approved if no prior instructions were provided.

Secondly, the policies are not uniform, they have their own rules regarding access, deletion, and retention. Some might allow limited access to accounts while others permit only memorialisation without data download thereby creating inconsistency, confusion<sup>19</sup> especially where a person has multiple digital accounts across different platforms.

Thirdly, the rules being contractual and governed by terms of service are non- negotiable and rarely read by an individual. Families generally do not have a say in one sided company policies with no right to challenge the rules or unfair refusals or delays. The personal data decisions are left to corporate discretion rather than a rule of law.

Fourthly, the policies do not address the cyber crime risks and they do not prevent misuse of digital footprints. Their focus is limited to managing accounts, not protecting identity or dignity after death

---

<sup>18</sup> Edina Harbinja, *Digital Death, Digital Assets and Post-mortem Privacy* (Edinburgh University Press 2022) 143–168.

<sup>19</sup> Edina Harbinja and Tatjana Papić, 'Post-mortem Privacy 2.0' (2018) 28 *Information & Communications Technology Law* 203.

Therefore, a corporate tool cannot be a substitute for a comprehensive legal framework. Voluntary corporate goodwill should not be the sole criteria to protect digital dignity, privacy, and autonomy.

## VI. DIGITAL ORPHANS BEYOND BORDERS: AN INTERNATIONAL LEGAL PERSPECTIVE

Unlike India, several other jurisdictions have started recognising the fact that the digital data does not simply disappear upon the death of a person and have started acknowledging the problem and providing legal solution.

As of 2026 **China** legally recognises digital assets such as social media accounts, cryptocurrency and online gaming items as personal property which can even be inherited under the Civil Code<sup>20</sup>. Close relatives may also access, copy or delete a deceased person's data for their own "lawful and legitimate interests" provided the deceased did not arrange otherwise.

**Estonia** provides a highly structured system where a person's consent for data processing remains valid for 10 years after death (or 20 years for a minor). Heirs can authorise data processing within the statutory period if it aligns with the deceased's original intent<sup>21</sup>.

**United States**- over 40 states have adopted the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)<sup>22</sup>. The law allows legally appointed fiduciaries such as executors and guardians to access digital accounts of deceased, subject to privacy safeguards. Just like bank accounts or property, the law treats digital assets as part of estate planning.

The General Data Protection Regulation (GDPR)<sup>23</sup> of the **EU** allows members to enact national legislation managing personal data after death, but it primarily protects living individuals. **France** and other nations have benefited from this flexibility by allowing people to specify how their personal data should be stored, deleted, or communicated after death<sup>24</sup>.

Additionally, it enables family members to contact service providers with specific demands

---

<sup>20</sup>Civil Code of the People's Republic of China, 2020, arts 127, 1122–1123.

<sup>21</sup> Personal Data Protection Act (Estonia), 2019, § 9.

<sup>22</sup> Revised Uniform Fiduciary Access to Digital Assets Act, 2015 (Uniform Law Commission).

<sup>23</sup> Regulation (EU) 2016/679 (General Data Protection Regulation), art 2(1), recital 27.

<sup>24</sup> French Data Protection Act (Loi Informatique et Libertés), art 85 (as amended 2016).

pertaining to data. Following a historic decision in 2018<sup>25</sup>, **Germany** allows digital accounts to be passed on to heirs under the universal succession principle, treating them like tangible letters. Although they are unable to actively utilize the deceased's social media accounts, heirs typically get controlled access to them.

The idea of **digital wills**, which allow a person to specify how their internet accounts and digital data will be treated after death, has already started to gain recognition in some nations<sup>26</sup>. Even deleting accounts, transferring photos, designating a **digital executor**, and more may be included in the instructions.

The concept of a person's legal and social legacy is strengthened by legal acknowledgment, as opposed to viewing it as an identity that companies control after death. It balances the individual's privacy and liberty with the demands and rights of the surviving family members. Indian law does not yet explicitly recognize posthumous digital rights or fiduciary access to digital data. Families are forced to rely on the unclear platform agreements and policies due to the gap. As India expands its AI-driven services and digital governance, the absence of a legal framework for digital death becomes risky.

## VII. FROM LEGAL VACCUM TO LEGAL VISION: THE ROAD AHEAD

Current legal framework sees privacy as a right that ends at death whereas technology does not work that way- the data is present forever. This gap between the law and the technology leaves families susceptible and helpless. It puts digital dignity at risk for the next innovation. The protection of the law must not only be limited to the lives but it must be extended beyond death to ensure that an individual is not resurrected without consent.

Like the moral rights in copyright law, which protects the identity and integrity even after the author's death, the digital posthumous personality rights should be legally protected against any misuse, distortion, exploitation, unauthorised access, or simulation. Such recognition would enable the courts and regulators to protect these rights without getting into the complexities involved with survivability of personal rights.

---

<sup>25</sup> Bundesgerichtshof (Federal Court of Justice), Judgment of 12 July 2018, Case No III ZR 183/17.

<sup>26</sup> Edina Harbinja, *Digital Death, Digital Assets and Post-mortem Privacy* (Edinburgh University Press 2022) 211–240.

At present, companies exercise discretionary control over the management of account, driven by contracts rather than obligations. Imposition of mandatory “digital death” protocol to stop processing, using, collecting the deceased data for training the AI, restriction on sharing the data to a third party and prevent any identity authentication tools such as biometrics to remain active. A mandatory reporting of any suspicious activity linked to the account of the deceased to the cybercrime authorities thereby shifting the primary responsibility from the families to institutions situated in a better position to prevent any compromise with the data.

Indian succession law must evolve to recognise digital assets and identity. Digital executor or digital nominee must be introduced, allowing individuals to legally appoint someone to manage their online accounts, cloud storage, crypto wallets, and AI profiles. The instructions must be binding in nature and enforceable through legal processes.

The cyber laws have yet not been able to catch up with the AI advancement and its misuse with personal identities. Dead individuals can be resurrected using clone voices and usage of deepfakes to gain undue advantages or emotionally manipulate the relatives. It is not merely frightening but also dangerous. When such data use used for any form of fraud, political manipulation or psychological exploitation, the law should treat it as a serious crime and hold offenders strictly liable.

Policy must be adopted whereby a mandatory disclosure must be required that an interaction involves AI generated representation of a deceased individual. Explicit consent must be required by the individual to use his data such as images, voice, behaviour pattern for AI based usage.

Digital platforms, cybercrime units, and the Data Protection Board must clearly coordinate at the institutional level. Digital abuse can be considerably reduced by requiring the mandatory reporting of questionable activity and providing a quicker redressal procedure. Further, a redressal mechanism can be adopted under the current laws to provide a time bound remedy for account freezing, data deletion. Without a well framed enforceability mechanism, the law continues to remain merely on the books.

Citizens are expected to be active protectors rather than passive observers until such improvements are implemented. People should retain crucial passwords, notify trusted family

members about digital assets and subscriptions, and proactively activate legacy contacts and account nomination features on internet platforms.

Protecting digital dignity requires both legal reform and responsible digital behaviour. Until Parliament steps up to treat dignity, identity, and memory as important as it is in life, citizens must become a first line of defence against the misuse of digital data.

## VIII. CONCLUSION

Where the traditional legal framework treat death as an end to the personality and privacy the digital ecosystem goes on to store, use, process, exploit, monetise the digital data indefinitely. The continued digital presence even after biological life has distorted the idea of law in the context of memory and technology. This distortion leaves the individuals and families vulnerable without any effectual; legal redressal thereby creating a class of digital orphans whose identities are digitally present without any legal guardian.

Indian law addresses the cyber harms only post misuse and no structured mechanism is offered to prevent posthumous data protection. The corporate platform policies are not substitutable to the legal recognition because they are driven by corporate incentives rather than privacy and dignity protection. India is placed at a digitally disadvantageous situation in the absence of any statutory legal framework aligning to digital inheritance, fiduciary access, and deletion rights.

The concept of dignity needs evolution in the light of constitutional and human rights perspective whereby it is protected as an element of human dignity even post death. When the identity continues to persist in the digital sphere, the law cannot restrict it to the biological boundaries alone. Right to digital rest, right not to be digitally resurrected, exploited, misused, or misrepresented after death should be understood as a natural extension of the essential constitutional principles.

With rapid digitisation, AI deployments and developing digital public infrastructure, the absence of posthumous data protection laws will leave the individuals and eventually the institutions to ethical, legal crisis. The concept of constitutional democracy and the principle

of dignity will be severely undermined by the lack of recognition in the era of technological advancement.