



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Posthumous Personality And Data Protection: Safeguarding Digital Legacies.

Asst. Prof. Dhanashri Yogesh Kadam

Assistant Professor,

Bhagubai Changu Thakur College of Law, New Panvel, Maharashtra

Prof. (Dr.) Kalpana V. Jawale

Professor, PG Department of Law,

Sant Gadge Baba Amravati University, Amravati, Maharashtra

Abstract

The exponential growth in digital technologies has generated a hybrid system that lays the groundwork for complex physical and virtual identities. From the moment of their birth-and increasingly even before-babies start leaving their digital footprints from one processor to another, from one platform to another, and from one service provider to another. Such footprints can be anyone ranging from social media profiles to cloud-based archives, biometric identifiers, geolocation histories, algorithmically generated likenesses, and AI recreations to the human personality: digital self. The death of the physical body is not considered death for the digital self; a digital personality continues to exist in the form of stored data traces, memorialized profiles, communications, data traces, and even synthetic reproductions.

This raises many complex legal, ethical, and philosophical questions about the persistence of identity beyond biological death. Who has authority over the digital assets of the deceased? May their image or likeness be commercialized without their consent? Can the "right to be forgotten" transcend the death of the right-holder? And what limits, if any, should be attached to the resurrection of a person's voice, face, or personality through artificial intelligence?

Significant development in the recognition of personality rights and data protection regulations has occurred for the postulation of dignity, autonomy, and privacy of the living. The posthumous legal treatment of these rights is much more fragmented, nascent, and, in numerous scenarios, non-existent. Jurisdictions vary widely as regards whether such rights survive death, for how long, and whether they can be enforced by heirs or executors. The lack of an apt wholesome framework leaves those digital legacies vulnerable to misuse, ranging from deepfake porn and identity theft to unauthorized commercialization of the late celebrity's image.

This paper presents some of the major conceptual and jurisprudential ideas to recognize and protect posthumous personality rights in the digital domain, ranging from several by-law philosophies, such as the Natural Rights Theory, considering those rights conferred on a human being as correlated with dignity, and therefore, could not die with him or her; Roscoe Pound's Theory of Interests, wherein the law takes into consideration the balance

among individual, social, and public interests; and the Theory of Justice of John Rawls, according to which the framework of justice should be generated under conditions that are fair and impartial so as to sustain equality.

Keywords - Posthumous rights, digital personality, data protection, digital legacy, Digital Personal Data Protection Act 2023.

I. Introduction

Such is the enormity of change created by another view of data generation in the splitting of the human from the digital world through the twenty-first century. Every online activity—whether a social media post, search query, biometric scan, or voice recording—contributes to the development of a digital self: a collection of data about the individual, personal expressions, and identifiers floating alongside and increasingly entwined with the corporeal self. This change in data generation has created a mark in perpetuity—a data trace that sometimes is not lost even with the physical demise of the person for whom the life data indicatesⁱ.

After death, varying degrees of individual personality embed themselves into the digital domain: memorialized social media profiles, archived e-mails, cloud photo albums, stored biometric profiles, and hologram likenessesⁱⁱ. This often-called digital afterlife, has formed this very unique interstice of law, technology, and ethics. It brings along its own set of issues: Who has rights over the data of a deceased? Should their image, likeness, or voice be commercially exploited after death? Can a consent given in life relate to death? Should the "right to be forgotten" survive its holder at deathⁱⁱⁱ?

In principle, existing laws were to protect the rights and interests of living persons. Personality rights involve protecting one's name, image, likeness, and reputation, and they usually lapse upon death unless otherwise provided by statute^{iv}. Similarly, post-death data protection is largely viewed as a nonissue, with usable data protection laws, including the E.U.'s General Data Protection Regulation (GDPR)^v and India's Digital Personal Data Protection Act, 2023^{vi}, coming to the rescue of only living persons in a timely manner. Such legislative silence leaves a vacuum where digital posthumous persona could be exploited.

The consequences of the said gap are serious indeed. Should nothing intervene, posthumous digital identity becomes provider-rejected reproduction identity theft deepfake manipulation^{vii}. It leads to commercial exploitation sans consent for celebrities and public figures from the posthumous commercial application of likeness^{viii}. In the case of ordinary people, it means risking the perpetuation of personal information in ways that could be against their own dignity and beliefs or the will of their families^{ix}.

The paper considers these problems by contemplating the conceptual and jurisprudential bases for granting posthumous personality rights in the digital sphere. Resorting to Natural Rights Theory, which considers dignity to be inherent and timeless^x; Roscoe Pound's Theory of Interests, which seeks a balancing of individual, group, and societal interests^{xi}; and Rawls' Theory of Justice, which calls for fairness behind a veil of ignorance^{xii}. Through comparative legal analysis—covering the European Union, the United States, India, and Australia—it analyzes the existing frameworks, noting deficiencies, and then proposes a model for protecting digital legacies.

Amongst other things, the study intends to sustain a somewhat fledgling and thus under-explored area of the law that is bound to become a matter of greater urgency as technology further extends human identity temporally.

With philosophical justifications serving as a background, the paper tries to assess the existing codifications insofar as they are in force in selected jurisdictions and to identify some good practice, some lacunae, and some divergences that might be of use. By intertwining jurisprudential reasoning with the comparative law analysis, the paper will proceed to the crystallization of a proposed model legal framework that might be able to address the particular issues in the digital afterlife precisely in an attempt to see that the rights, dignity, and wishes of a person be respected beyond death in the rising digital world.

II. Conceptualizing Posthumous Personality in the Digital Age.

Personality rights—sometimes referred to as the “right of publicity” or “personality interests”—are legal protections accorded to an individual’s identity and distinctive attributes. Traditionally, these encompass an individual’s name, image, voice, likeness, signature, and reputation, shielding them from unauthorized exploitation or misrepresentation. Their core function is to preserve a person’s control over the commercial and reputational use of their persona during their lifetime^{xiii}.

Posthumous personality rights are an extension of this legal protection beyond death. They aim to safeguard the integrity, dignity, and sometimes the economic value of a deceased person’s identity, typically empowering the estate, legal heirs, or designated representatives to authorize or prohibit uses of the deceased’s persona. Historically, such rights were primarily invoked in contexts involving celebrities, historical figures, or public personalities whose images continued to generate commercial value posthumously—examples include disputes over the commercial use of Marilyn Monroe’s image or Albert Einstein’s likeness.

Yet, digitalization has greatly transformed the scope and relevance of the posthumous personality. The lines that once separated the celebrities from the “ordinary” ones have become blurred, with billions of persons creating immortal digital personalities that continue to exist after they have physically ceased to exist. These personalities entail not only carefully put-together public images but also private archives stored in cloud services, semi-public profiles, and datasets embedded within machine-learning systems.

B. Digital Dimensions of Posthumous Personality

A post-mortem personality in modern times crosses the traditional rights of publicity and blends into data protection, intellectual property, tort law, privacy, and the ethics of emerging AI. In a digital jurisdiction, these include:

2.1. Social Media Accounts and Digital Content

Profiles, pictures, posts, or messages on social media sites such as Facebook, Instagram, Twitter/X, and LinkedIn are usually accessible after an individual’s demise. They can be memorialized or deleted on request; however, with no legal recognition of posthumous personality, any request made could go unenforced by the family.

2.3 Biometric Data

Facial templates, iris scans, and fingerprints stored in a database could potentially reside for eternity. The characterization of biometric identifiers is explicitly precluded in the law is absent; in such cases, these could be duplicated or misused for impersonation or deepfakes.

2.3. AI-Impersonation or Voice Clones

Powerful generative AI tools can now recreate a deceased person's face, likeness, or voice to create new content, sometimes for honorable commemorative use, but with a possibility for commercial or political persuasion, and without a mechanism to secure consenting use beyond a person's lifetime, their dignity could be violated through these processes.

2.4. Email and Cloud Archives

Personal correspondence, documents, or digital media is sometimes located in email accounts and cloud-based systems (e.g., Google Drive, iCloud) raises issues of access and control. Service provider contracts often treat email mailboxes, and documents as licenses that are typically nontransferable, and may limit the rights of survivors to inherit or manage them.

In contrast to physical property, digital identity does not degrade or disappear over time. Digital identity can be copied without limit and altered, used, or monetized without consent. The permanence, replicability, and alterability of digital assets create novel risks –

- a) Identity Misappropriation – using the image or voice of the deceased for advertising, or even political or entertainment messaging, without approval;
- b) Deep fakes exploitation – creating harmful, false, or defamatory content using the deceased's identity;
- c) Data mines – accessing and monetizing personal data from dead accounts for the purposes of analytics and targeted advertising; and
- d) Cultural / emotional injury – injuring the memory and dignity of the deceased, and affecting their family's moral interests.

A coherent definition of posthumous personality in the digital era must, therefore, combine traditional dignity-based protections with principles of data governance. to account for implications of individual property rights in both moral rights (ie, harms to reputation, dignity) and economic rights (i.e., commercialization, licensing) in a global, borderless digital space.)

III. Key Concerns

The safeguarding of post-mortem rights, as they arise in parts of the digital context, raises a set of intertwined legal and ethical issues. First, there is the matter of privacy and the public interest at stake; in particular, there is the difficulty in deciding how long such rights will attach after death. Some states, such as California, grant individuals rights that last for a period of up to seventy years after death; others are silent and, therefore, leave uncertainty and inconsistency of enforcement. The real question is one of balance—the actor's dignity (rest in peace), the emotional and economic safety of their heirs, and the rights of others to utilize the person's likeness, voice, or image in situations of cultural, historical, or artistic value. Relatedly, is the enterprise of consent and autonomy—should the consent someone manifests during life extend indefinitely into and after death? Digital service providers such as Facebook and Google now provide legacy settings allowing those who create an account to 'request' the deletion of their account or request the service provider memorialize their account, but these functions tend to operate as contractual devices and would be harder to enforce against competing claims from heirs or from competing claims by corporate actors.

The philosophical and legal difficulty is determining if a person can still have autonomy over their personal data and digital identity after they die, given the newer technology that can artificially and (often without permission) recreate a person's voice, likeness, or expressions. The third major concern is jurisdictional issues. Digital assets often exist in multiple jurisdictional contexts at the same time, implicating different legal regimes of privacy, intellectual property, and succession law. For example, the General Data Protection Regulation (GDPR) of the EU provides individuals with strong privacy rights while alive but leaves posthumous protections to the discretion of Member States - but France states that they provide some moral rights even after death. Without international harmonization, it is possible that “data havens” will develop where a person's posthumous persona can be misappropriated under weak regulatory regimes.

IV. India – Digital Personal Data Protection (DPDP) Act, 2023.

The DPDP Act, 2023, introduces a revolutionary process—the right to nominate—allowing a Data Principal to appoint a trusted person who can assume their rights (such as access, correction, erasure and grievance redress) to their data in the event of the death or incapacitation of the Data Principal. Under the section, as soon as the Data Principal dies or becomes incapacitated, the nominated person can act in the place of the Data Principal—only to the extent of what the Data Principal could have done under the Act and the rules^{xiv}.

The rights to appoint a nominee is further bolstered by Rule 13 of the DPDP Rules 2025 (currently being formulated) which requires Data Fiduciaries to create clear and accessible process mechanisms—like easy-to-use digital forms—for Data Principals to appoint a person. This would allow the nominee to be actionable and enforceable posthumously. In established Indian legal precedent, privacy rights are not inheritable. Courts have concluded that rights like privacy, publicity, and personality usually come to an end with the individual's death,

and cannot be passed to heirs or legal representatives. Note that the DPDP Act represents a clear deviation: the nomination made in accordance with Section 14 does not create inheritable rights; instead, it creates a limited fiduciary-like role for the nominee to handle, and if necessary deactivate or delete, the deceased's data in accordance to the Data Principal's wishes. This is similar to a digital executor's privileges when dealing with data-related matters, without providing property rights of the data itself.

Section 14 of the Digital Personal Data Protection Act, 2023, which empowers a Data Principal to designate another person to take on their rights upon death or incapacity, is plagued with considerable lacunae as it relates to posthumous data protection. To begin, it is an entirely opt-in provision, where the protection relies on the Data Principal assigning a nominee. There is no default provision in the law to clarify and to determine any person to control or request deletion of the deceased's personal data, in the absence of an assignment—that is, no legal heirs or executors, nor data will not be under-accessed. Secondly, the Act is silent on the time period posthumous rights may be exercised, meaning that there is no clarity, and this opens up the possibility of data fiduciaries having unregulated and varying practices for retaining or deleting data. An additional facet of this provision that is void of any review is cross-border issues; importantly, there is no indication of whether the nominee's authority would extend to data housed on servers outside of India, and if it does, how such authority would intersect with foreign data protection regimes such as the GDPR. Procedurally, there is no express requirement to substantiate a Data Principal's death nor any procedure for verifying the identity of the nominee, which creates the possibility of fraud or impersonation. Further, this section provides a limited discussion of personal data without discussion of whether nominees are entitled to manage access to digitally associated asset and services (i.e. a cryptocurrency wallet, social media account or subscription services) which typically comprise a significant part of a digital legacy. The Act does not establish an override framework when the nominees' instructions conflict with statutory requirements or considerations of public interest and it does not establish rules to deal with appointing multiple nominees or disputes between nominees.

V. Gaps and Challenges

The legal protection of the digital persona of the deceased is fraught with systemic problems. The primary problem is jurisdictional inconsistency. Some jurisdictions have limited posthumous personality rights in relation to a deceased person's data or likeness; others completely lack any recognized form of such protection, thus allowing for the risk of inconsistent protections in a borderless digital landscape. This is exacerbated when a digital asset or data is located on servers in multiple countries. The rapid advancement of technology adds a sense of urgency to the mix. The recent developments in deepfake pornography and scams using synthesized voices, as well as the ability to make AI-generated "holograms" of the deceased, present opportunities for misuse that existing rights are poorly equipped to regulate. Enforcement poses a different set of challenges. It can be difficult to ascertain the appropriate jurisdiction(s) or applicable law when data is spread across borders and under the control of a multinational corporation. There are also ethical ambiguities to resolve, as they require a balancing act between respecting the preferences and dignity of the deceased, recognizing the emotional interests and rights of heirs, and considering the broader public interest in issues like historical preservation and artistic and free speech pursuits. Collectively, these barriers bring to light the need for a clear and coherent cross-border, forward-thinking legal framework to regulate posthumous personality rights in the digital age.

VI. Proposed Recommendations

6.1. Statutory Recognition of Posthumous Digital Rights

Government should consider legislation, either through amending the Digital Personal Data Protection Act, 2023, or through a separate legislation, specifically recognition of deceased individuals' rights to their digital personality, which includes name, likeness, image, voice and personal data, for however long, say twenty (20) years post death.

6.2. Incorporation of "Digital Wills"

"Digital Wills," which are legally recognized, should be passed into law so that a person can give legally binding directions during life for whether others have the right to manage, share, delete, or memorialize their digital assets once they die.

6.3. Appointment of a Digital Estate Executor

The law must have provisions for a digital executor who has been appointed to manage a deceased person's digital assets, as well as take on fiduciary responsibilities and comply with the deceased's wishes as well as the law.

6.4. Posthumous Right to be Forgotten

There should be posthumous "right to be forgotten" provisions in law whereby legal representatives can request deletion or anonymization of data where consent for continued usage has not been given by the deceased.

6.5. Cross-Border Enforcement Mechanisms

Additionally, India should enter into bilateral or multilateral agreements, specifically in terms of our data rights even after we die, to provide a manner of mutual recognition of posthumous data rights, where it aids in cooperating across jurisdictions, when the data is stored on foreign servers.

6.6. Protection Against Technological Exploitation

Explicit prohibitions ought to be established on creating or reproducing deepfakes, AI-generated likenesses or synthetic voices of dead persons without lawful consent.

6.7. Public Awareness and Capacity-Building

Awareness programs should inform people of their options with regard to their digital legacy, whilst capacity building activities should educate legal practitioners, technology companies and executors responsible for enforcing post-mortem rights.

VII. Conclusion

The lack of explicit statutory protections for posthumous digital personality rights in India presents significant legislative gaps in an era where, the digital persona has economic, emotional and cultural value, both to the individual and others. Although the Digital Personal Data Protection Act, 2023 is an important step towards protecting privacy, the law's terminological silence surrounding the rights in terms of deceased persons means that this data is exposed for misuse, technological exploitation and conflict of jurisdiction. Without standardization, heirs, attorneys, or service providers must work either with separate and inconsistent contractual terms, or face complicated legal situations across jurisdictions.

Honoring posthumous digital rights extends far beyond preserving privacy beyond death; it encompasses dignity, autonomy, and upholding the digital self. In order to avoid ethical breaches such as deepfake manipulation, the exploitation of Artificial Intelligence for identity resurrection, and commercial exploitation of someone's likeness, a regime that incorporates the autonomy of the deceased, the rights of heirs, and legitimate interests of society must be articulated. By talking about statutory recognition with express consent, developing regulatory frameworks in the form of digital wills, establishing a duty to act with skill and care as the deceased's legal representative, and including multilateral legal mechanisms to mutually enforce legislation around digital rights, India can create a strong, robust regime that is future resistant. Doing so would not only help to protect individual legacies but align Indian law alongside forward-thinking global standards and principles, by ensuring the principles of justice, respect, and accountability governs the digital afterlife.

REFERENCES

- ⁱ Luciano Floridi, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* 55–60 (2014)
- ⁱⁱ Edina Harbinja, Post-Mortem Privacy 2.0: Theory, Law, and Technology, 31 *Information & Communications Tech. L.* 1, 3–4 (2022).
- ⁱⁱⁱ *Id.* at 6.
- ^{iv} See Melville B. Nimmer, The Right of Publicity, 19 *Law & Contemp. Probs.* 203, 211–12 (1954).
- ^v Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 3, 2016 O.J. (L 119) 1.
- ^{vi} The Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
- ^{vii} Joshua A.T. Fairfield, BitProperty, 88 *S. Cal. L. Rev.* 805, 810–12 (2015).
- ^{viii} See *Martin Luther King Jr. Ctr. for Soc. Change, Inc. v. Am. Heritage Prods., Inc.*, 296 S.E.2d 697 (Ga. 1982).
- ^{ix} See Naomi Cahn, Postmortem Life On-Line, 25 *Prob. & Prop.* 36, 37–39 (2011).
- ^x John Locke, *Two Treatises of Government* 287–90 (Peter Laslett ed., Cambridge Univ. Press 1988) (1690).
- ^{xi} Roscoe Pound, *An Introduction to the Philosophy of Law* 90–92 (1922).
- ^{xii} John Rawls, *A Theory of Justice* 11–17 (rev. ed. 1999)
- ^{xiii} See Jennifer E. Rothman, *The Right of Publicity: Privacy Reimagined for a Public World* 85–87 (
- ^{xiv} Act No. 22 OF 2023, Sec.14, India code.

