Digital Death: Legal Rights of Digital Avatars and Posthumous Data

Dr. Swarup Mukherjee
Associate Professor of Law, ICFAI University Tripura

***Abstract*—The rapid expansion of artificial intelligence, immersive virtual worlds, and data-driven ecosystems has transformed the boundaries of human identity, giving rise to a new dimension of existence: the digital self. Individuals today cultivate extensive online footprints—ranging from social media profiles and cloud archives to AI-trained personal assistants and interactive digital avatars. As these digital manifestations increasingly mirror human personality, preferences, and behaviour, the question of what becomes of such digital traces after biological death has emerged as a critical issue in contemporary legal discourse. This article investigates the evolving concept of digital death by analysing the legal, ethical, and doctrinal challenges associated with posthumous digital existence. It interrogates the legitimacy and scope of rights that may be claimed by or on behalf of digital avatars, including personality rights, autonomy, and protection against misuse or unauthorized simulation. Further, it examines the status of posthumous data under privacy law, intellectual property regimes, and succession frameworks, highlighting inconsistencies across jurisdictions. Drawing on comparative jurisprudence, platform governance policies, and emerging scholarship on digital personhood, the article proposes guiding principles for a coherent legal architecture that safeguards human dignity, autonomy, and identity in an era where individuals may continue to "exist" digitally long after their physical lives end.**

***Index Terms*—Digital Death; Posthumous Data Rights; Digital Avatars; AI Personhood; Digital Estate; Posthumous Privacy; Data Protection; Personality Rights; Digital Legacy; Digital Succession; AI Resurrection; Griefbots; Metaverse Identity; Likeness Rights; Deepfakes; Platform Governance; Digital Dignity; Posthumous Autonomy; Virtual Personhood; Digital Self; Privacy After Death; Digital Asset Management; Digital Will; Technological Personhood; Digital Afterlife Regulation.**

I. INTRODUCTION

The boundary between life and death has blurred in the digital age. Social media memorial pages, AI-based "griefbots" that simulate deceased individuals, and interactive holographic personas are altering the social experience of death and remembrance. At the same time, digital estates—containing photos, communications, intellectual property, cloud-stored assets, and AI-trained models—outlive the individual and exist as autonomous entities governed by platform terms of service rather than statutory law.

The central legal question is: Does the digital self possess rights after biological death? If so, who controls those rights, and to what extent? Traditional succession law, which governs physical property and testamentary dispositions, is poorly equipped to address issues such as the continued operation of a deceased person's AI avatar, the commercial use of their likeness in metaverse environments, or the privacy of posthumous data stored on foreign servers.

II. CONCEPTUAL FRAMEWORK: THE DIGITAL SELF AND DIGITAL DEATH

2.1 The Digital Self as an Extension of Personhood

In contemporary digital environments, the self is no longer confined to biological existence or physical presence. Modern technologies—ranging from social media platforms and cloud storage to advanced machine-learning systems—enable individuals to create rich, multidimensional digital identities. These include:

a. Identifiable Data

This encompasses basic personal information such as names, photographs, contact details, and biometric markers. Such data is often dispersed across multiple platforms and is regulated by privacy and data

protection laws. It forms the core of digital identity because it connects real-world identity with digital presence.

b. Expressive Content

Individuals routinely generate creative and expressive outputs online: writings, videos, artwork, intellectual commentary, and social interactions. This material functions as a digital footprint of personality, values, beliefs, and emotional life. It also raises questions of copyright ownership and moral rights after death.

c. Behavioural and Predictive Data

Advances in data analytics allow platforms to capture and store behavioural patterns—purchase histories, browsing trajectories, interpersonal relationships, sleep cycles, and even emotional reactions. Over time, this data allows AI systems to construct predictive models of a person. Such data has immense commercial value yet remains poorly addressed by legal frameworks.

d. AI-Generated Avatars

The most complex layer of digital personhood is the AI-driven avatar. These systems may use personal data to replicate speech patterns, decision-making tendencies, and emotional responses. In some cases, they can continue to evolve through machine learning, even after the individual's death. This creates a fundamentally new entity: a semi-autonomous digital persona that outlives biological life and challenges traditional notions of identity, authorship, consent, and liability.

Theoretical Implications

The digital self-results in an expanded notion of personhood where identity is not merely corporeal but multilocational and data-driven. As such, legal systems must reconsider whether rights—traditionally tied to human biological existence—should extend to digital manifestations that survive death.

2.2 Defining Digital Death

Digital death does not simply mean the cessation of biological life but refers to the continuity, transformation, or fragmentation of digital identity after physical death. Key dimensions include:

a. Data Persistence

Unlike physical belongings, digital data does not naturally degrade. Emails, social media posts, cloud-stored documents, AI models, and cryptocurrency wallets may persist indefinitely unless deleted. This persistence challenges legal doctrines that assume property naturally transitions upon death.

b. Loss of Control

Upon death, individuals no longer exercise agency over how their data is used, interpreted, or monetised. Without clear legal directives, this creates a vacuum that platforms often fill, making unilateral decisions regarding memorialisation, deletion, or data retention.

c. Continued Digital Activity

Automated systems—such as scheduled posts, subscriptions, AI assistants, or autonomous avatars—may continue to operate after the user's death. Some avatars may continue to generate content or interact with others, creating an eerie form of posthumous "life."

d. Emotional and Social Consequences

Digital remnants of a deceased person have social impacts on family, friends, and the public. For example, misuse of a deceased individual's image or the creation of deepfakes can cause psychological trauma, defamation, or manipulation of historical memory.

Legal Implications

Digital death exposes gaps in existing laws, including:

- the absence of posthumous privacy rights in many jurisdictions,
- unclear status of digital assets under succession law,
- platform-governed data control instead of state regulation, and
- lack of consent mechanisms for posthumous use of digital likeness.

Digital death therefore marks a paradigm shift requiring modern legal systems to redefine how identity, privacy, and autonomy continue or terminate beyond biological existence.

III. LEGAL STATUS OF POSTHUMOUS DATA

3.1 Data as Property vs. Data as Personality

The core legal debate is whether personal data should be treated as property, capable of inheritance and transfer, or as an aspect of personality, which traditionally ends with death.

a. Data as Property

Under the property framework, data is an asset that can be:

- transferred through a will,
- accessed by legal heirs, and
- protected from unauthorised use.

Several U.S. states have adopted the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), which empowers executors to access digital assets subject to platform policies. Courts in China have treated social media accounts and digital photographs as inheritable assets. This model simplifies succession but risks commodifying identity.

b. Data as Personality

In many jurisdictions, personal data is tied to dignity and autonomy, not economic value. The GDPR, for example, protects personal data as a fundamental human right. However, because it applies only to living persons, posthumous data exists in a legal vacuum unless national laws fill the gap. Personality-based frameworks argue that personal dignity does not cease at death and that misuse of posthumous data can harm the memory or reputation of the deceased.

c. Hybrid Approaches

Legal scholars increasingly propose a hybrid model combining:

- property rights for assets with economic value, and
- personality rights for sensitive or expressive data.

This approach acknowledges the unique nature of digital identity, which cannot be neatly classified as either a commodity or a purely personal attribute.

3.2 Posthumous Privacy

Posthumous privacy refers to the right of individuals to have their personal data protected even after death.

a. Why Does Posthumous Privacy Matter?

Posthumous data can include highly sensitive information:

- medical records
- intimate messages
- biometric data
- political or religious views
- private photographs

Misuse can harm not only the deceased's dignity but also their family's emotional and social well-being.

b. Current Legal Position

Globally, posthumous privacy lacks uniform protection:

- France allows heirs to control deceased persons' data.
- Italy extends certain privacy rights beyond death.
- India, UK, and USA largely extinguish privacy rights upon death unless specific statutes or platform policies apply.

This inconsistency creates uncertainty, especially for transnational digital assets.

c. Posthumous Reputation and Dignity

Historically, defamation law in many countries does not protect the dead. However, digital content is permanent and quickly disseminated, so false or harmful statements made posthumously can distort public memory. There is growing academic consensus that reputational protection must extend beyond death.

d. Practical Challenges

- Who decides what the deceased would have wanted?
- Should families have unrestricted access to private communications?
- Can platforms deny heirs access citing user confidentiality?
- How should data be treated when stored in multiple jurisdictions?

These unresolved questions highlight the need for explicit statutory regimes.

IV. DIGITAL AVATARS AND THE QUESTION OF LEGAL RIGHTS

4.1 Typology and Evolution of Digital Avatars

Digital avatars have evolved from simple graphical icons to sophisticated AI-driven entities capable of learning, adapting, and interacting autonomously. Understanding their legal nature requires distinguishing between key categories:

a. Static Legacy Avatars

These include memorialised social media profiles, digital photo albums, archived emails, or frozen accounts that do not evolve after the user's death. While static, they still raise important concerns related to access, deletion rights, and the rights of families.

b. Interactive Avatars

Examples include chatbots built using the deceased's text messages, voice notes, and email history. These avatars simulate conversations and emotional responses, often serving as grief-support tools. Their legal status is complex because they replicate personality traits and speech patterns, thereby implicating likeness, privacy, and consent issues.

c. Autonomous AI Avatars

These advanced avatars can:

- Generate new content,
- Participate in virtual platforms,

- Enter into digital transactions,
- Adapt to new information.

An autonomous avatar may continue to produce outputs that influence real people, raising questions about accountability, authorship, and the continuity of digital identity.

Legal Importance of Classification

The degree of autonomy determines whether the avatar should be treated as:

- Property,
- Intellectual creation,
- An extension of personality, or
- A new legal entity deserving limited rights.

This distinction is crucial for designing laws on ownership, consent, liability, and posthumous protection.

4.2 Do Digital Avatars Possess Legal Rights?

The legal debate surrounding avatar rights encompasses multiple possibilities:

a. Avatars as Property (No Independent Rights)

Under the conventional view, digital avatars are simply digital assets owned by the user or the user's estate. They are treated like artworks or software. This approach is efficient but deeply flawed when applied to expressive, behaviourally rich AI avatars that bear personal resemblance to the deceased.

b. Avatars as Embodiments of Personality (Derivative Rights)

As avatars often contain representations of personality, emotions, and behavioural patterns, they can be viewed as an extension of the human self. Thus, rights protecting identity, dignity, and likeness should continue to apply posthumously.

c. Avatars as Semi-Autonomous Digital Agents (Functional Rights)

A growing school of cyber-jurisprudence argues that highly autonomous avatars may require limited legal rights such as:

- the right not to be altered, manipulated, or deleted without legal authority;
- the right to maintain integrity;
- the right to attribution for content they generate.

These are not "human" rights but rather functional legal protections, similar to rights granted to corporations or animals for specific purposes.

4.3 Key Legal Questions Arising from Avatar Rights

1. Who owns the avatar after death? The estate? The platform? The family?
2. Does the avatar have the right to exist, or can heirs delete it?
3. Who is responsible for harmful statements made by an autonomous avatar?
4. Can avatars enter into contracts in metaverse environments?
5. Should avatars be allowed to "live" indefinitely?

Current legal systems provide no consistent answers.

V. POSTHUMOUS CONTROL: OWNERSHIP AND GOVERNANCE OF DIGITAL REMAINS

5.1 The Role of the Estate in Managing Digital Assets

In most jurisdictions, physical and intellectual property passes to legal heirs through traditional succession law. However, digital assets complicate this framework because:

- Many online accounts are governed by licensing agreements, not ownership.
- Platforms often claim exclusive control over digital content.
- Succession laws generally do not recognise data stored on foreign servers.

Challenges for Executors and Legal Heirs

- Inability to access accounts due to passwords and encryption.
- Conflicts with platform Terms of Service (ToS).
- Fragmented data across multiple jurisdictions.
- Disputes over whether digital content can be inherited at all.

Executors frequently face more resistance from private corporations than from family members, demonstrating the imbalance between private digital governance and formal legal structures.

5.2 Family Rights, Cultural Norms, and Posthumous Autonomy

The ethics of posthumous digital identity vary widely across cultures. In many societies, remembrance and control over the deceased's legacy are deeply rooted in familial traditions. Families may seek:

- Access to personal messages for closure,
- Preservation of photographs for cultural continuity,
- Deletion of content that might cause social embarrassment,
- Control over the deceased's image to avoid misuse.

However, this may conflict with the deceased's own digital autonomy. For example:

- A deceased person may wish their data to be deleted, but family members may prefer memorialisation.
- Conversely, a person may wish for their avatar to continue, but the family considers it emotionally distressing or culturally inappropriate.

Legal systems must therefore balance individual autonomy, family rights, and public interest, a complex triad rarely addressed in existing statutes.

5.3 Platform Power and Private Digital Governance

A defining feature of digital death is the dominance of private companies in regulating the digital afterlife.

Platform-Driven Mechanisms

- Facebook: memorialisation, legacy contacts, but limited access to messages.
- Google: Inactive Account Manager allowing limited pre-death choices.
- Apple: Legacy Contact feature with strict privacy controls.

These mechanisms prioritize platform interests and global data policies over local laws or moral considerations.

The Problem of Privatised Afterlife Governance

- Platforms function as de facto lawmakers.
- Users remain bound by contracts they seldom read.
- Cross-border servers make local enforcement difficult.
- Corporate policies may override the deceased's autonomy or family rights.

This raises the urgent need for state intervention to reclaim regulatory authority from private entities.

VI. EMERGING ISSUES: AI, METAVERSE, AND BIO-DIGITAL IDENTITY

6.1 AI "Resurrection" Technologies and the Question of Consent

AI resurrection refers to recreating a digital version of a deceased person using algorithms trained on personal data. Examples include griefbots, digital clones, and voice-replicating systems.

Key Ethical and Legal Questions

- Did the deceased give consent during their lifetime?
- Should implicit consent (e.g., public posts) be allowed?
- Can families override the deceased's privacy to create an avatar?
- Who controls the resurrected avatar—family, estate, or platform?

Without clear legal rules, consent often defaults to platform discretion or family demands, risking misuse.

Risks of Non-Consensual Digital Resurrection

- Emotional exploitation
- Posthumous defamation
- Identity distortion
- Commercial monetisation of the deceased
- Manipulation of survivors' emotions

Therefore, a robust legal framework must require explicit, informed, and revocable consent for the creation of posthumous AI avatars.

6.2 Digital Likeness Rights and the Deepfake Problem

Deepfakes and AI-generated likeness are now so realistic that distinguishing genuine content from fabricated material has become difficult. The dead are especially vulnerable because they cannot defend themselves.

Key Legal Concerns

- Unauthorised use of voice, face, or personality
- Posthumous defamation through fabricated content
- Exploitation of deceased celebrities for profit
- Misleading portrayals affecting public memory
- Manipulation in political or social contexts

Some jurisdictions protect celebrity likeness posthumously for 20–70 years, but such laws often exclude ordinary individuals, creating a dangerous legal gap.

6.3 Metaverse Personhood, Virtual Economies, and Persistent Avatars

In metaverse environments, avatars may continue to perform activities after the user's biological death. These include:

- Owning virtual property
- Entering into smart contracts
- Generating income
- Creating artistic content
- Interacting with other avatars

New Legal Challenges

1. Ownership of Virtual Assets: Who inherits virtual land, NFTs, or in-game currency accumulated by the avatar?

2. Autonomy of Persistent Avatars: If an avatar continues to function autonomously, is shutting it down a form of digital "death"? Who authorises this?
3. Legal Capacity and Accountability: Should avatars be allowed a form of "operational personhood" to validate contracts, transactions, or creative rights?
4. Cross-Jurisdictional Issues: Metaverse platforms exist outside conventional borders, making regulation difficult.

As AI-driven avatars become more independent, the law will face unprecedented questions regarding digital agency.

VII. COMPARATIVE LEGAL APPROACHES

Regulation of digital death varies significantly across jurisdictions. This comparative overview highlights how different legal systems conceptualise posthumous data rights, digital estate management, and avatar governance.

7.1 United States

The U.S. framework is fragmented due to the absence of a unified federal privacy law. States follow varying models, with the most prominent being the **Revised** Uniform Fiduciary Access to Digital Assets Act (RUFADAA).

Key Characteristics

- RUFADAA gives executors limited access to digital assets but prioritises platform Terms of Service.
- Access is tiered:
  - Content-level data (emails, messages) requires explicit user consent.
  - Metadata and records can be accessed by fiduciaries unless restricted.
- Several states recognise posthumous publicity rights, particularly for celebrities (e.g., California, Tennessee).
- Courts increasingly treat digital assets as inheritable property, especially in cases involving photos, emails, or cryptocurrency.

Limitations

- No consistent protection for posthumous privacy of ordinary individuals.
- Platform dominance over inheritance and memorialisation remains strong.
- AI avatars and digital resurrection technologies remain largely unregulated.

7.2 European Union

EU law is anchored in dignity-based data protection principles, making it more progressive in conceptualising posthumous digital rights.

Key Features

- GDPR applies only to living individuals but allows member states to legislate posthumous rights.
- France, Italy, Estonia, and Denmark have adopted varying degrees of posthumous privacy protections.
- Certain jurisdictions permit heirs to:
  - Manage the deceased's online accounts
  - Request erasure of data
  - Control digital legacies

Strengths

- Strong cultural emphasis on individual dignity and moral rights.
- Greater willingness to extend privacy principles beyond death.
- Some countries explicitly regulate digital inheritance.

Weaknesses

- Inconsistent protections across member states.
- No uniform legal framework for AI avatars or deepfake misuse after death.
- Platform policies may still override user wishes.

7.3 China

China's courts and regulators have shown increasing attentiveness to digital estate issues, often favouring the rights of families.

Key Trends

- Courts recognise digital assets (photos, e-wallet balances, chat logs) as inheritable property.
- Strong state control over data helps centralise regulatory oversight.
- Succession Law is interpreted broadly to ensure families can access digital remains.

Advantages

- Clearer recognition of digital inheritance rights.
- Greater judicial willingness to compel platforms to provide access.

Challenges

- Limited privacy protections, both pre- and posthumous.

- Strong state control raises concerns about over-reach, especially in accessing private digital content.

7.4 India

India currently lacks a dedicated legal framework for digital death.

Key Features

- The Digital Personal Data Protection Act, 2023 (DPDPA) protects only the living.
- No statutory mechanism for digital wills, posthumous data rights, or avatar protection.
- Courts have expanded privacy for the living (Puttaswamy) but remain silent on digital afterlife.
- Platform terms dominate digital legacy governance.

Urgent Gaps

- Lack of posthumous privacy law
- No recognition of digital inheritance
- No regulation of AI avatars or deepfake misuse
- Absence of legal obligations on platforms regarding memorialisation or deletion

India is poised for significant legislative development in this domain.

VIII. DOCTRINAL CHALLENGES

Digital death exposes deep structural limitations in traditional legal doctrines. Existing frameworks governing privacy, succession, personhood, and liability were designed for a physical world and struggle to adapt to the complexities of digital identity.

8.1 The Succession Law Gap

Succession law traditionally governs tangible assets and certain intangible rights (copyrights, debts, securities). Digital assets challenge this system in several ways:

a. Licensing vs. Ownership

Most digital platforms provide only a licence to use content. After death, the licence extinguishes, leaving nothing to inherit.

b. Passwords and Encryption

Digital assets may be inaccessible despite legal entitlement. Without encryption keys, estates cannot manage or delete digital remains.

c. Cross-Jurisdictional Servers

Digital assets stored globally complicate enforcement of local succession laws, leading to conflicts of law.

d. Non-Transferable Data

Some data—such as behavioural analytics, algorithmic profiles, and predictive models—may be considered non-transferable due to platform ownership.

Thus, succession law in its classical form is inadequate for the digital era.

8.2 Personality Rights and Posthumous Identity

Personality rights typically include rights to reputation, privacy, dignity, and likeness. These are traditionally tied to biological life.

Challenges

- Digital identity continues to shape public memory after death.
- Avatars can mimic speech or behaviour, affecting how society perceives the deceased.
- Deepfakes can distort historical truth.

The doctrine must evolve to recognise that digital personality does not end with physical life but survives in data form—potentially indefinitely.

8.3 Jurisdictional Conflicts and Cross-Border Data

Digital platforms routinely store data on international servers. Posthumous rights therefore face:

- Conflicts of law (which country's law governs digital remains?)
- Platform-to-platform inconsistencies
- Difficulty enforcing national laws extraterritorially

These conflicts make it nearly impossible for heirs to enforce rights consistently.

8.4 Ethical and Moral Dilemmas

The digital afterlife raises profound ethical questions:

a. Manipulating the Dead

Using AI to simulate or speak for the deceased without consent violates human dignity and personal autonomy.

b. Emotional Harm to the Living

Unwanted exposure to digital remnants or AI avatars can impede grief and psychological recovery.

c. Distortion of Historical Memory

Deepfakes or manipulated avatars may alter collective memory, shaping false narratives about individuals.

d. Commodification of Personality

Treating digital likeness as a commercial asset risks reducing human identity to economic value.

The law must balance autonomy, dignity, and public ethics.

IX. TOWARDS A LEGAL FRAMEWORK FOR DIGITAL DEATH

A future-ready legal framework must address the conceptual, procedural, and ethical dimensions of digital identity after death.

9.1 Statutory Recognition of Posthumous Data Rights

Legislation must ensure:

- Protection of digital dignity after death
- Restricted use of sensitive posthumous data
- Clear guidelines for deletion, retention, and inheritance
- Remedies for misuse (e.g., deepfakes, avatar manipulation)

Such rights should apply to all individuals, not only public figures.

9.2 Digital Estate Planning and Consent Mechanisms

Just as wills manage physical estates, digital wills should legally authorise individuals to specify:

- What happens to online accounts
- Whether avatars may be created or continued
- How digital assets are inherited
- Whether data may be archived, deleted, or memorialised

Consent must be explicit, informed, and legally binding.

9.3 Regulation of AI Avatars and Digital Clones

Governments should enact clear rules requiring:

- Consent before creating or operating AI replicas
- Transparency in avatar behaviour and data usage
- Prohibitions on unauthorised simulations
- Accountability for harmful or defamatory avatar actions
- Limits on the commercial use of posthumous avatars

This prevents misuse while preserving autonomy and dignity.

9.4 Platform Accountability and Governance Reform

Platforms must be legally compelled to:

- Provide transparent digital death policies
- Honour user directives in digital wills
- Allow heirs meaningful access to data that is legally inheritable
- Delete data upon lawful request
- Prevent non-consensual resurrection or likeness misuse

Further, platforms should not be allowed to override statutory rights with unilateral contracts.

9.5 Protection of Likeness and Image After Death

Posthumous personality rights—including image, voice, and likeness—must be protected through:

- Anti-deepfake statutes
- Penalties for unauthorised commercial exploitation
- Dignity-based rights extended beyond biological death
- Uniform laws that protect both celebrities and private individuals

Such protection ensures that digital identity cannot be misappropriated.

X. CONCLUSION

The phenomenon of *digital death* marks one of the most profound legal frontiers of the 21st century. As human identity becomes increasingly intertwined with digital ecosystems—through social media, metaverse platforms, AI-driven avatars, and posthumous data—the law must evolve to safeguard dignity, autonomy, and rights beyond physical mortality. Digital avatars, whether static profiles or dynamic AI simulations, now function as extensions of personality. Posthumous data, meanwhile, acquires emotional, economic, and social value that affects families, platforms, and even the broader public sphere.

Current legal systems remain largely unprepared. Most jurisdictions treat digital death through fragmented frameworks—data protection laws that cease at death, intellectual property norms that do not fully embrace AI-generated identity, and estate laws that rarely include virtual selves. This legal vacuum generates risks of misuse, commodification, impersonation, and unauthorized "digital resurrection." At the same time, it raises pressing ethical dilemmas around consent, ownership, inheritance, and the preservation of human dignity.

To address these challenges, legal reform must follow three guiding principles:

i. Posthumous Autonomy: A deceased individual's preferences regarding their digital afterlife—whether to delete, memorialize, transfer, or simulate—must be treated with the same respect as their physical remains and personal legacy. Digital wills or consent-based frameworks should be legally mandated.

ii. Digital Dignity and Protection:Avatars and posthumous data must be shielded from exploitation, deepfake manipulation, and unauthorized replication. Legislators must expand personality rights to include the digital persona, enforceable even after death.

iii. Platform Accountability and Governance**:** Technology companies must adopt transparent policies for digital death, supported by statutory obligations, including notification duties, access rights for families, and limits on AI-driven uses of deceased users' data.

Ultimately, digital death is not merely a technological issue—it is a question of identity, personhood, and the social meaning we attach to memory and legacy. As AI advances and metaverse environments blur the line between human and avatar, the law must safeguard these emerging forms of existence. A coherent, rights-based legal framework will ensure that digital life—and digital afterlife—honors human dignity and prevents the erosion of personal rights in a world where individuals may continue to "exist" long after their biological lives end.

REFERENCES

[1] Baron, J., & Hill, J. (2018). Privacy and Security in the Digital Afterlife: Managing Data Beyond Death. Harvard Journal of Law & Technology, 31(2), 1–46.

[2] Bell, A. (2020). Deadbots and Digital Ghosts: AI, Grief, and the Law. International Journal of Law and Information Technology, 28(3), 233–255.

[3] Beverley-Smith, H. (2023). Personality Rights in the Digital Age. Oxford University Press.

[4] Calvert, C. (2021). Deepfakes, Identity, and Posthumous Rights of Publicity. Journal of Intellectual Property Law, 28(1), 45–78.

[5] Capurro, R. (2017). Digital Personhood: Ethical and Legal Dimensions. Ethics and Information Technology, 19(1), 5–15.

[6] European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Official Journal of the European Union.

[7] Facebook (Meta). (2020). Memorialization Settings & Legacy Contact Policies. Meta Transparency Center.

[8] Ghosh, S. (2021). Death, Data and Dignity: A Comparative Study of Posthumous Privacy Rights. NUJS Law Review, 13(2), 134–161.

[9] Harbinja, E. (2013). Does the Digital Afterlife Need New Law? The Emergence of Posthumous Personality Rights. Queen Mary Journal of Intellectual Property, 3(1), 24–37.

[10] Harbinja, E. (2017). Post-Mortem Privacy 2.0: Revisiting the Regulation of Personal Data after Death. Scripted Journal, 14(2), 1–29.

[11] Kasket, E. (2019). All the Ghosts in the Machine: The Digital Afterlife of Your Personal Data. Robinson/Little, Brown.

[12] Koops, B.-J., & Leenes, R. (2020). Born Digital and Born Again Digital: Posthumous Data Protection. Computer Law & Security Review, 36, 105367.

[13] Mendoza, I., & Bygrave, L. A. (2017). Data Protection and the Right to Privacy after Death. International Data Privacy Law, 7(3), 122–134.

[14] Purtova, N. (2019). The Law of Everything: Broad Conceptualization of Personal Data. International Data Privacy Law, 10(2), 1–52.

[15] Shyam, N. (2020). Digital Assets and Succession Law in India: A Need for Reform. Indian Journal of Law and Technology, 16(1), 47–85.

[16] Solove, D. J. (2021). Understanding Privacy in the Age of AI. Yale Law Journal Forum, 130, 345–370.

[17] UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence.

[18] Wright, J., & Schultz, J. (2022). Avatars, AI-Simulated Identities, and Emerging Questions of Digital Personhood. Stanford Technology Law Review, 25(1), 92–131.

[19] Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.