International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Unnominated Nominees and Digital Legacies: Evaluating India's Legal Framework for Postmortem Privacy and Proposing Comprehensive Reforms

Jayashree A[1], Kamali R[2]

[1,2]Student, SASTRA Deemed University, Tanjore

ABSTRACT:

In an era where our lives are increasingly intertwined with digital technology, what happensto our digital identities and personal data after we pass away? This paper delves into the pressing issue of postmortem privacy in India, exploring the legal and ethical complexities that arise in managing personal data after death. With the rise of digital assets, such as government documents stored on platforms like Digilocker and personal information on social media, the need for a comprehensive regulatory framework is more critical than ever.

Focusing on the Digital Personal Data Protection Act (DPDP), the research highlights its inadequacies in addressing the intricacies of digital asset management, particularly in cases where individuals have not designated a nominee. This lack of clear guidelines leaves sensitive information vulnerable, potentially resulting in disputes among surviving family members over access and control of digital legacies.

Additionally, the paper examines international frameworks, such as the RUFADA Act from the USA, drawing parallels and insights that could inform reforms in the Indian context. By critically analyzing existing legislation and proposing necessary legal reforms, this study advocates for a robust framework that safeguards individuals' digital legacies and upholds their privacy rights posthumously. Ultimately, this research seeks to contribute to the evolving discourse on digital rights and privacy, emphasizing the urgency of developing effective regulatory measures to navigate the complexities of our digital lives in the age of information.

KEYWORDS: Post-Mortem Privacy, Digital Legacy, Unnominated Digital Asset, Privacyrights

CHAPTER - 1

1.1 Introduction

People in the digital age depend more and more on digital platforms to store and manage a variety of personal assets and information, such as government documents, social media accounts, and financial records. Digilocker, a government-backed program, is one of the key platforms in India for securely storing vital digital information[1]. Social networking sites such as Facebook, Instagram, and Twitter also act as archives for private messages, memories, and other digital identities. Although these platforms

[1] https://www.digilocker.gov.in/

provide many benefits while a person is still alive, they also bring up difficult questions about postmortem privacy and what happens to these digital assets when someone passes away, especially if no candidate has been chosen tomanage their data after their death.

Postmortem privacy refers to the safeguarding and administration of a person's personal information, social media profiles, and other digital assets after death[2]. In India, the legal framework controlling such matters is still immature, with no particular legislation addressingunnominated digital assets on platforms such as Digilocker or major social media networks. This legislative loophole frequently creates confusion about a person's digital legacy, potentially leading to unwanted access, loss of sensitive information, or disagreements amongsurviving family members.

Social media platforms, in particular, present unique challenges. These accounts often contain intimate data, conversations, photos, and videos that reflect a person's life and identity, raising questions about who has the right to access, manage, or delete this data after the account holder's death. The lack of clear legal guidelines not only risks infringing on the deceased's privacy but also complicates the process for family members or executors trying to manage or retrieve these assets

This paper explores the pressing need for regulations on unnominated digital assets in India, with a focus on both government-backed platforms like Digilocker and widely used social media platforms. It delves into the existing gaps in the legal framework surrounding postmortem privacy and advocates for comprehensive regulatory measures that ensure the proper management of digital legacies, balancing privacy rights with practical considerationsfor surviving family members.

1.3 RESEARCH PROBLEM

In the digital era, post-mortem privacy has become a pressing concern, particularly as existing legal frameworks do not adequately address the intricacies of managing personal data after an individual's death. The Digital Personal Data Protection Act (DPDP) includes provisions in Section 26 that allow individuals to designate a person to manage their data posthumously. However, notable deficiencies in this legislation remain. It does not provide guidance on the status of personal data for those who have not appointed a nominee, resultingin a lack of privacy safeguards for deceased individuals. Furthermore, the act fails to establishclear criteria for selecting nominees, raising questions about whether preference should be given to immediate family members or if broader nominations should be permitted.

Additionally, the rights conferred to nominees concerning different categories of data are notexplicitly defined, creating challenges in balancing individual privacy with public interests. As digital footprints continue to linger indefinitely, there is a crucial need for significant reforms to enhance legal protections for post-mortem privacy and ensure that individuals'data rights are respected even after death.

1.4 RESEARCH OBJECTIVE

1. To evaluate the adequacy of India's Digital Personal Data Protection Act (DPDP) in safeguarding post- mortem privacy, particularly in cases where no nominee is appointed.
2. To analyze international legal frameworks, such as the RUFADA Act from the USA, and explore their applicability in addressing post- mortem pry issues in India.
3. To propose legal reforms that address the gaps in India's DPDP Act, specifically regarding the management of unnominated digital data after death.

1.5 RESEARCH HYPOTHESIS

The lack of specific guidelines in the Digital Personal Data Protection Act (DPDP) regarding the

[2]https://www.sciencedirect.com/science/article/pii/S0267364922000802#:~:text=Such%20post%2Dmortem%20privacy%20would,and%20digital%20footprints%20more%20generally.

nomination process for managing a deceased person's data results in inconsistent protection of post-mortem privacy rights in India.

1.6 RESEARCH QUESTION

1. How does the Digital Personal Data Protection Act (DPDP) in India address post-mortem privacy, particularly for digital assets of individuals who have not appointed a nominee?
2. What legal gaps exist in India's current framework regarding the management of un- nominated digital assets after death?
3. How can international frameworks, such as the RUFADA Act from the USA, be adapted to improve India's approach to post-mortem privacy?

CHAPTER II

2.1. RESEARCH METHODOLOGY

In this research paper, we have adopted a doctrinal research methodology. This approach focuses on the analysis of existing legal texts, statutes, case law, and relevant secondary sources to explore the complexities of postmortem privacy and the management of digital assets in India. By examining primary sources such as the Digital Personal Data Protection Act (DPDP) and judicial decisions, alongside secondary sources including legal journals, reports, and academic articles, we aim to identify gaps in the current legal framework and propose necessary reforms.

Now, we are going to look at postmortem privacy in detail, investigating its significance, challenges, and the legal implications of managing digital assets after death. This method allows for a comprehensive understanding of the legal principles governing digital legacies, facilitating informed recommendations for enhancing privacy protections in the digital age.

2.1.1. Post-Mortem Privacy: Concept and its Significance

Planning for the death of an account holder is challenging since there's no way to pinpoint an exact date. However, concerns about data ownership and privacy after death are very real.

Policymakers face a custodial challenge when managing clients' accounts after incapacity or death. Who bears the responsibility for safeguarding a user's data privacy and distributing digital assets after they pass away? What rights does an individual have over their digital assets when they can no longer manage them or when they are deceased?

In recent decades, the concept of privacy has broadened as societal expectations evolve, with each generation questioning the nature and importance of privacy. While we can acknowledge that "privacy is fundamental to our identity as human beings," its interpretation varies depending on the individual and institution. Although definitions continue to shift and most organizations prioritize privacy policies for the living, there is often little focus on policies concerning the death of an account holder.

According to the International Association of Privacy Professionals., "Privacy is now a necessity of doing business,"[3] and any organization that engages with clients online will eventually need to address the handling of digital assets after incapacity or death, if they haven't already. The growing number of deceased users on Facebook has raised public awareness, emphasizing that a person's wishes after death matter not only to them but also to their grieving families and beneficiaries. Organizations with an online presence or those that handle an individual's data or digital assets must have privacy policies for handling the data of incapacitated or deceased account holders.

Post-mortem privacy refers to the management and protection of an individual's personal data, digital

[3] https://iapp.org/news/a/the-birth-of-postmortem-privacy

assets, and privacy rights after their death. As people increasingly rely on digital platforms for communication, storing memories, and managing assets, the question of what happens to this information after they die has become a significant concern. Post-mortem privacy addresses the legal, ethical, and practical issues surrounding the ownership, access, and control of a deceased person's digital presence and data.

One of the key arguments against recognizing post-mortem privacy is that the deceased cannot experience harm or injury, as they are no longer .The following analysis challenges this view, drawing a comparison to the right to bequeath property. Using a similar reasoning, it could be argued that the deceased should not care about what happens to their property after death, as they are no longer affected by its distribution. However, the interests at play here extend beyond just the family and society in terms of wealth distribution, as the right to dispose of property is upheld in most legal systems, even when it conflicts with the desires of heirs or societal expectations. This argument proposes that individuals do indeed have a stake in what happens after their death, especially in the digital realm, where the vast amount of personal data shared online and the significance of digital assets in shaping one's online identity make posthumous interests even more crucial than in the physical world Consequently, principles similar to those governing testamentary freedom over physical property should be adapted for digital environments, covering digital assets and personal data.

Yet another argument against the idea of privacy after death is that a person's legal life ends when they die, and with it, their legal rights, including privacy. However, Prof. Naffine points out that legal personality (a person's legal rights) isn't fixed—it can change depending on the type of law or legal system[4]. In this discussion, we are focusing on the legal personality of individuals (natural persons), not companies or organizations. There isn't a clear answer as to when someone's legal personality truly ends. In some cases, like with a will, a person's legal rights extend after death, allowing them to decide how their property is distributed.

Prof. Jonathan Turley challenges the idea that legal personality ends with death, arguing that we don't really know exactly when a legal person begins or ends. He suggests that physical death shouldn't automatically mean the end of someone's legal rights, since a will lets a deceased person control what happens to their property.

This argument connects to theories from Hegel and Radin, who say that property is a part of a person's identity (or personhood) and is necessary for developing that identity. So, just as property can be managed after death through a will, a person's identity continues in a way after death. In copyright law, the creator's personal rights (known as moral rights) continue after they die, lasting as long as the economic rights to the work exist, or even longer in somecases, like in France.

This evidence supports the idea that certain aspects of a person's identity—such as their dignity, integrity, and autonomy—can survive death, and if legal rights extend beyond death in these cases, then privacy should too.

2.1.2. Rights of the Dead in India: A Legal and Privacy Perspective

The legal framework surrounding the rights of deceased persons has long been debated in various contexts, from property inheritance and burial rituals to organ donation. However, with the rapid advancement of digital technology, the issue of privacy rights posthumously, particularly concerning digital data, has gained significant relevance. In India, this area remains underexplored, with gaps in

[4] https://research-management.mq.edu.au/ws/portalfiles/portal/16873759/mq-10857-Publisher+version+%28open+access%29.pdf

legislation such as the Digital Personal Data Protection Act (DPDP Act) of 2023[5]. While the act recognizes the need for nomination of data management in cases of incapacitation or death, it falls short in addressing certain critical aspects, particularly post-mortem privacy rights and consent related to digital data after death.This research explores these gaps and argues for a more robust legal framework to protect therights of dead persons.

i) The Right to Dignity and Privacy After Death

The Indian judiciary has recognized that the rights of individuals do not entirely cease upon death. In the landmark case of Parmanand Katara, Advocate v. Union of India & Anr. (1989)[6], the Supreme Court held that the right to dignity under Article 21 of the Constitution of India extends to a person even after death. The court ruled that the body of a deceased person mustbe treated with respect and dignity, in line with cultural and religious traditions.

However, this judgment, while progressive, primarily addresses the physical treatment of the dead and does not explicitly discuss digital privacy or the handling of a deceased person's personal information. Extending the concept of dignity to digital data is a necessary step in today's context, where the personal information of individuals is often stored and processed even after death.

ii) Post-Mortem Privacy and the Theory of Rights

The debate on post-mortem rights often revolves around two legal theories: will theory and interest theory.

Will Theory: This theory suggests that rights are tied to an individual's capacity to make choices. Since a dead person cannot exercise choices, proponents of this theory argue that they cannot have rights after death. Under this view, the concept of posthumous digital privacy would be dismissed, as the deceased cannot actively manage or decide on their digitalinformation[7].

Interest Theory: This theory, on the other hand, argues that individuals have rights based on their interests, even if they cannot actively assert them. For example, living persons often express wishes about what should happen to their body or belongings after death. These wishes provide peace of mind and fulfillment to the living, and it is the duty of the legal system to honor them. Applying this theory to digital privacy, individuals should have the

right to pre-consent how their digital data is handled after death, thereby protecting their privacy and ensuring their data is treated in accordance with their wishes[8].

In many legal systems, while it is commonly accepted that dead persons do not have legal rights, efforts are still made to respect their wishes regarding property, burial, and other matters. By analogy, post-mortem digital privacy should be safeguarded in a similar manner

2.1.3. Informational self determination

The term informational self-determination was first used in a German constitutional court case in 1983. The case known as the Census Act Temporary Injunction Case ,dealt with the use of the information collected in the Census by the German state. This farsighted judgement articulated the need to understand information as a facet of an individuals' personality and related to human dignity; giving her the right to choose what information, how much and where such information may be shared or disclosed or used by the State. Thus, making the concept of informational privacy a much more wholesome

[5] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[6] https://indiankanoon.org/doc/498126/
[7] https://www.jstor.org/stable/3504897
[8] https://eprints.whiterose.ac.uk/211364/3/Bowen%2C%20The%20Interest%20Theory%20of%20Rights%20at%20the%20Margins.pdf

concept than the right to be forgotten or the right to data protection. Informational determinism envelops these rights and is a dynamic concept capable of adapting to the increasingly fast past methods of collecting information personal to an individual. This concept then acts as a counterpoint to the individuals' expectation from the state to share all the data or information it has on its citizens.[9]

The worlds' first comprehensive privacy law on informational privacy, it is widely agreed, was in the German state of Hesse. Both Germany and the USA have been active in this field of rights but while Germany has now a clearly recognised link between the constitution andthe protection of this right (after the 1983 case the Federal Data Protection Act of Germany was modified to include the constitutional mandate) the links in US privacy law are not so well defined**.**

2.1.4. RUFADAA as a Model: Shaping India's Digital Asset Management

The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) was developed inresponse to the growing complexities surrounding the management of digital assets after death or incapacity. As more personal, financial, and professional activities shifted online, traditional estate laws struggled to address the growing importance of digital assets, such as social media accounts, email, cloud storage, and cryptocurrency. This left estate executors and fiduciaries with significant legal and practical challenges in managing these assets.

Before RUFADAA[10], there were substantial obstacles to accessing a deceased or incapacitated person's digital assets. Privacy laws, such as the Electronic Communications Privacy Act (ECPA)[11] and the Stored Communications Act (SCA)*[12]*, were designed to protect the privacy of individuals but inadvertently prevented estate representatives from accessing digital communications without explicit consent. Additionally, terms of service agreements (TOS) for online platforms often restricted third-party access, leaving families and fiduciaries unable to manage or retrieve digital assets without facing legal or policy-based hurdles[13].

In 2014, the Uniform Law Commission (ULC) introduced the Uniform Fiduciary Access to Digital Assets Act (UFADAA) to give fiduciaries the same authority over digital assets as they have over physical property[14]. This act aimed to allow fiduciaries, such as executors or guardians, to manage digital accounts after a person's death or incapacity. However, the UFADAA faced opposition from major tech companies and privacy advocates, who argued that it conflicted with privacy laws and violated user agreements by allowing fiduciaries to access private digital communications.

As a result, the ULC revised the act, resulting in the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), which was finalized in 2015. RUFADAA aimed to balancethe need for fiduciaries to access and manage digital assets while respecting the privacy of the account holder and the terms of service agreements.

One of the key principles of RUFADAA is **user control**. It prioritizes the account holder's wishes in determining what happens to their digital assets after their death. If a user has utilized an online tool provided by a service (such as Google's Inactive Account Manager or Facebook's Legacy Contact) to designate someone to manage their digital assets, those instructions will take precedence over any other

[9] https://theleaflet.in/specialissues/informational-self-determination-its-origin-and-some-context-by-lavanya-regunathan-fischer/
[10] https://trustandwill.com/learn/what-is-rufadaa?srsltid=AfmBOoqMxQbmTptUn2HwPk9wP2KdUhfqj1-NdOkfe-mgjKfpJoXYNhQ4
[11] https://www.sciencedirect.com/topics/computer-science/electronic-communications-privacy-act-of-1986
[12] https://crsreports.congress.gov/product/pdf/LSB/LSB10801
[13] https://platformglossary.info/terms-of-service/
[14] https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22

directives, such as those in a will. This ensures that the individual's express preferences regarding their digital assets are respected.

In cases where no specific instructions are left by the account holder, **terms of service agreements** of online platforms will determine how digital assets are handled. RUFADAA recognizes the importance of these agreements, allowing service providers to retain control over access to accounts, in accordance with their privacy policies and user contracts.

However, if no such terms are available or applicable, fiduciaries may seek court supervision to gain access to digital assets that are essential for administering the estate.

RUFADAA also places **limitations on access** to protect the deceased person's privacy. Fiduciaries are only granted access to digital assets that are necessary for estate management, and access to private communications, such as emails, is restricted unless the deceased had explicitly authorized it. This balance ensures that fiduciaries can fulfill their responsibilities without infringing on the privacy of the deceased individual.

The **Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)** in the United States provides a robust framework for managing digital assets after death, including provisions for handling situations where no nominee has been designated. This act can serve as an inspiration for India's Digital Personal Data Protection Act (DPDP), particularly in addressing the gap surrounding **unnominated entries** — situations where a deceased person has not appointed a nominee to manage their digital assets.

2.1.5. Reference from RUFADAA and Application to Indian Context:

Under RUFADAA, clear procedures are outlined for fiduciaries (such as executors of estates or court-appointed guardians) to access a deceased individual's digital assets when no explicit nominee has been designated. This ensures that the digital presence of a person is managed responsibly, even in the absence of pre-emptive instructions. By contrast, India's DPDP Act, while allowing individuals to nominate someone to manage their data after death, **does not provide any clarity on how to handle digital assets if no nominee is appointed**.

India could benefit from incorporating a similar provision from RUFADAA into its legal framework, establishing guidelines for managing **unnominated digital entries**[15]. This would ensure that personal data is not left unprotected or vulnerable to misuse in the absence of a designated nominee. For instance, the law could stipulate that in the absence of a nominee, the responsibility could automatically fall to the closest family members, or alternatively, a legal representative could be appointed by the courts to manage the data in a manner consistent with the deceased person's privacy preferences and legal rights.

Customization for Indian Law:

While taking inspiration from RUFADAA, the Indian law should adapt these procedures to account for local cultural and legal norms. For instance:

1. **Priority of Nominees**: RUFADAA gives fiduciaries access to digital assets, but the Indian framework might prioritize immediate family members first, with a fallback to court-appointed guardians if no family members are available.
2. **Handling Sensitive Data**: Indian law could introduce more specific rules about the types of data accessible to these fiduciaries or family members, ensuring that sensitive personal data is handled with care and protecting the deceased's dignity and privacy even after death.
3. **Incorporation of Consent Principles**: A procedure could be introduced in the DPDP Act allowing individuals to pre-consent to how their digital assets should be handled, similar to how organ

[15] https://www.arenesslaw.com/digital-inheritance-law-that-secures-the-future-of-your-digital-assets/

donation operates. This would offer better posthumous control over one's digital identity.

By adopting and modifying the principles found in RUFADAA, **India could close the existing legislative gaps**, ensuring that digital assets are appropriately managed even in cases where no nominee has been appointed. This would strengthen post-mortem data privacy protections in India and align its laws with international best practices.

In the realm of digital privacy, the **Revised Uniform Fiduciary Access to Digital Assets Act (RUFADA)**, a legal framework from the United States, provides crucial guidance on handling digital assets after a person's death, particularly when no nominee or fiduciary has been appointed. This act ensures that in the absence of a nominated individual, there are clear procedures in place to manage the deceased person's digital assets. The **RUFADA**

Act allows a designated fiduciary to access and manage the digital accounts of a deceased person, thereby offering a structured approach to handling digital privacy even when no prior nomination has been made.[16]

In contrast, **India's Digital Personal Data Protection Act (DPDP)** currently provides individuals with the option to nominate someone to manage their digital data after death, as outlined in **Section 26**. However, the DPDP Act falls short of addressing what happens to the digital data of individuals who pass away without making such a nomination. There is no procedure in place to ensure that the personal data of these **unnominated entries** is handled with the same level of protection and dignity. This lack of clarity leaves a significant gap in the legal framework, potentially leading to data being misused, mishandled, or neglected afterdeath.

To address this gap, **India can take inspiration from the RUFADA Act** by incorporating provisions that clearly define the procedures for managing **unnominated data** after death. Such provisions could ensure that even if a person has not nominated someone, a legal mechanism exists to determine how their data should be managed, whether by immediate family members, court-appointed fiduciaries, or another legal process. Furthermore, a consent-based system could be introduced, wherein individuals are given the option to specify their preferences for the management of their data posthumously, similar to how organ donation consents are handled. This could be integrated into the user experience of digital platforms, allowing users to **pre-select options** that determine how their accounts and personal data should be treated after their passing.

This system would ensure that personal data continues to be safeguarded in line with the individual's wishes, even after their death, and would provide a robust framework for managing privacy, regardless of whether a nomination has been made. By adopting procedures from RUFADAA Act and adapting them to India's legal context, we can ensure that the **Digital Personal Data Protection Act** provides a comprehensive approach to **post mortem digital privacy**, ensuring that **unnominated entries** are handled with care and legalprecision.

CHAPTER - III

3.1 CONCLUSION

In the digital age, the issue of post-mortem privacy presents complex challenges that existing legal frameworks, such as the Digital Personal Data Protection Act (DPDP) 2023, do not fully address. The Act's provision under Section 26, which allows individuals to nominate someone to manage their

[16] https://easeenet.com/blog/what-is-rufadaa-and-why-should-you-care/

personal data after death, is a positive step toward recognizing posthumous data rights[17]. However, it does not comprehensively protect the privacy of those who pass away without appointing a nominee, leaving a significant portion of digital footprints unmanaged and vulnerable to potential misuse.

The absence of specific criteria for the selection of nominees is another significant gap, raising concerns about who should be entrusted with control over a deceased person's data. Should priority be given to next of kin, or should individuals have the flexibility to nominate others, such as friends or legal representatives, based on their specific preferences? This lack of clarity opens up possibilities for conflicts or misuse, particularly in cases where the deceased's wishes are unclear or contested.

Furthermore, the Act does not delineate the rights and responsibilities of nominees in managing different types of data, such as personal communications, financial records, or social media accounts. This ambiguity can lead to inconsistent interpretations and practices, creating uncertainty about how to balance the deceased's privacy rights with the legitimate interests of the public, family members, or legal authorities.

As digital footprints endure long after death, it becomes increasingly vital to ensure that the dignity and privacy of individuals are preserved. Internationally, several jurisdictions have begun to address post-mortem privacy more comprehensively, often incorporating provisions for pre-consent and more clearly defined rights for both the deceased and their appointed data managers. India's legal framework still lags behind in this regard, and adopting best practices from these jurisdictions could help strengthen posthumous data protection.

In conclusion, while the DPDP Act provides a foundation for addressing post-mortem privacy, it is clear that substantial reforms are necessary. By introducing explicit provisions for managing the data of individuals without nominees, establishing clearer criteria for selecting data managers, and specifying the extent of rights over different categories of data, India can ensure that privacy rights are respected even after death. Additionally, public awareness and education about these rights are crucial to making these protections accessible and effective. A more nuanced, comprehensive approach to post-mortem privacy will not only safeguard personal data but also honor the dignity of individuals beyond their lifetime.

3.2 SCOPE AND LIMITATIONS OF THE STUDY

This paper explores the legal framework surrounding postmortem privacy in India, specifically focusing on the Digital Personal Data Protection Act (DPDP) and its provisions for managing digital assets after death. It examines the implications of existing laws, highlights gaps in regulation, and discusses the applicability of international frameworks like the RUFADA Act. The research aims to propose legal reforms that enhance the protection of digital legacies while balancing privacy rights with practical considerations for surviving family members.

The study is limited to the analysis of current laws and frameworks within India, which may not encompass the broader implications of postmortem privacy in a global context.

Additionally, the research primarily relies on doctrinal analysis, and may not include empirical data or case studies that could provide further insights into the real-world impact of existing regulations. The evolving nature of digital technologies and practices may also present challenges in ensuring the relevance of proposed reforms over time.

CHAPTER IV

[17] https://indiankanoon.org/doc/198889191/

RECOMMENDATIONS AND SUGGESTION

In India, the current legal framework lacks clear guidelines regarding unnominated nominees for managing digital assets after an individual's death. To address this gap, we can draw inspiration from the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADA) from the USA. Implementing a similar framework with tailored modifications could significantly enhance the management of digital legacies in India.

The Digital Personal Data Protection Act (DPDP) allows individuals to nominate parties for managing their digital assets; however, it does not provide clear guidelines on who these nominated persons should be. This ambiguity can lead to confusion and disputes among surviving family members. More extensive research is needed to establish criteria for selecting nominees, ensuring that individuals can confidently choose appropriate persons tomanage their digital legacies.

Additionally, while the DPDP enables nomination, it lacks a clear consent mechanism for the deletion of accounts after death. This oversight can lead to the unwanted retention of personal information in the digital realm. Therefore, it is crucial to introduce advanced directives as an option. Individuals should be empowered to express their wishes regarding the management and deletion of their personal information before their death.

To facilitate this, the provision for writing a will that includes directives on digital asset management and consent for deletion of accounts should be integrated into the DPDP. Thisapproach would ensure that individuals have control over their digital legacies and can prevent the unintended preservation of their personal information after they have passed away.

Moreover, awareness campaigns should be initiated to educate individuals about their rights concerning digital assets and the importance of making explicit directives regarding their management. Legal aid organizations could play a vital role in this educational outreach.

Additionally, the government could consider establishing a centralized digital asset registry that allows individuals to record their nominations and directives, making it easier for executors or family members to manage digital assets post-mortem.

By adopting these suggestions, we can create a more robust legal framework that respects individuals' privacy rights and addresses the complexities of postmortem digital asset management, ensuring that personal wishes regarding digital legacies are upheld.

CHAPTER-V REFERENCES

1. https://www.scconline.com/blog/post/2023/10/24/beyond-the-grave-exploring-the- legality-of-posthumous-publicity-

rights/https://www.scconline.com/blog/post/2023/10/24/beyond-the-grave-exploring- the-legality-of-posthumous-publicity-rights/
2. https://www.legalserviceindia.com/legal/article-120-should-your-privacy-die-with- you-.html#google_vignette
3. https://www.sciencedirect.com/science/article/pii/S0267364922000802? cf_chl_tk= aYm9pbW.TCbBhvnEXvmV9J2iyfb7VS6A1ndsag4Y19o-1729434088-1.0.1.1-zSxXcV4Z6x45K4760FnDesOR1GtZoCGaadx8_Py73hE
4. https://www.lexdinamica.com/post/beyond-the-grave-navigating-post-mortem-data- privacy
5. https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1275116#d1e133
6. https://kb.osu.edu/server/api/core/bitstreams/0c0c01ef-7b68-4d5a-b414- 1454a84d7f17/content
7. https://kemlaurin.medium.com/have-you-given-thought-to-what-happens-to-your- digital-profiles-when-you-die-df76a75edcd3
8. https://theleaflet.in/specialissues/informational-self-determination-its-origin-and- some-context-by-lavanya-regunathan-fischer/
9. https://leginfo.legislature.ca.gov/faces/home.xhtml
10. https://trustandwill.com/learn/what-is-rufadaa
11. https://www.azleg.gov/legtext/52leg/2r/laws/0165.htm
12. https://www.uniformlaws.org/committees/community- home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22
13. https://www.sciencedirect.com/science/article/abs/pii/S026736490800166
14. https://blog.ipleaders.in/all-about-the-legal-rights-of-the-dead/
15. https://publications.aston.ac.uk/id/eprint/37748/1/Post_mortem_privacy_2_0_theory_law_and_technology.pdf
16. https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_2