

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi-Disciplinary  
Peer Reviewed

[www.ijlra.com](http://www.ijlra.com)

## **DISCLAIMER**

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

## EDITORIALTEAM

### EDITORS

#### **Dr. Samrat Datta**

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*



#### **Dr. Namita Jain**



*Head & Associate Professor*

*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*

*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrish Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*

## Mrs.S.Kalpna

Assistant professor of Law

*Mrs.S.Kalpna, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*



## Avinash Kumar



*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

## **ABOUT US**

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

# DIGITAL AFTERLIFE AND POST-MORTEM DATA RIGHTS IN INDIA

AUTHORED BY - ADITYA MISHRA & AKSHAT MISHRA  
National Law Institute University Bhopal

## **ABSTRACT**

The rapid digitization of personal, financial, and social assets in India has created a critical legal vacuum regarding post-mortem data rights, where over 850 million internet users accumulate valuable digital legacies including photographs, communications, cryptocurrency, and social media accounts that lack clear inheritance frameworks upon death. This research addresses the fundamental question of how Indian law should balance deceased persons' privacy rights with legitimate family access needs to digital assets, examining the inadequacy of existing constitutional privacy protections under Article 21, statutory provisions in the Information Technology Act 2000 and Indian Succession Act 1925, and the absence of judicial precedent governing digital inheritance disputes. Through comparative analysis of international frameworks, particularly the European Union's GDPR "right to be forgotten" provisions and the United States' Uniform Fiduciary Access to Digital Assets Act, this study demonstrates that viable legislative solutions exist for reconciling competing privacy and inheritance interests through tiered access systems, user control mechanisms, and platform compliance requirements. The research proposes a comprehensive Digital Inheritance Act specifically adapted for India's constitutional framework, diverse personal law systems, and technological infrastructure challenges, incorporating procedural safeguards that protect posthumous privacy while enabling reasonable heir access to digital assets for estate administration, memorial purposes, and family legacy preservation, ultimately arguing that immediate legislative intervention is essential to address growing disputes between families and digital service providers while establishing India as a global leader in digital inheritance law.

**Keywords:** Digital inheritance, post-mortem data rights, digital assets, posthumous privacy, succession law, cyber law

## I. Introduction

### A. Opening Statement and Context Setting

The digital revolution has fundamentally transformed traditional concepts of property and inheritance, creating unprecedented challenges for legal systems worldwide. In the contemporary digital ecosystem, property extends far beyond tangible assets to encompass vast repositories of personal data, digital communications, financial accounts, and creative works stored across multiple platforms and jurisdictions.<sup>1</sup> The conventional understanding of inheritance, rooted in physical assets and documented ownership, struggles to accommodate the intangible yet valuable nature of digital possessions that continue to exist in virtual space long after their creators have departed.

India's digital landscape presents a particularly compelling case study for examining these emerging legal complexities. As of 2025, India hosts over 850 million internet users, representing approximately 60% of the population, with digital penetration growing at an unprecedented rate of 12% annually.<sup>2</sup> The country's digital economy, valued at USD 200 billion, encompasses extensive use of cloud storage services, social media platforms, digital payment systems, and cryptocurrency exchanges.<sup>3</sup> This massive digital footprint inevitably translates into substantial posthumous digital asset accumulation, with an estimated 2.8 million social media accounts becoming memorialized annually due to user deaths.<sup>4</sup>

The concept of "digital afterlife" encompasses the continued existence and potential accessibility of an individual's digital presence after death, including all forms of data, accounts, and digital assets that persist on various platforms and servers.<sup>5</sup> This phenomenon extends beyond mere data storage to include ongoing digital interactions, automated systems, and the preservation of digital identity and reputation. Post-mortem data rights, conversely, refer to the legal entitlements and protections applicable to deceased individuals' digital information, encompassing rights of access, control, modification, and deletion that may be

---

<sup>1</sup> Natalie M Ohana, 'Digital Death and Afterlife: Issues and Approaches' in *Thanatosensitivity in Digital Humanities* (Routledge 2021) 15-32.

<sup>2</sup> Telecom Regulatory Authority of India, 'The Indian Telecom Services Performance Indicators Report' (TRAI 2025) 8.

<sup>3</sup> Ministry of Electronics and Information Technology, 'Digital India Programme: Annual Report 2024-25' (Government of India 2025) 23.

<sup>4</sup> Statista Research Department, 'Digital Death Statistics: India Social Media User Mortality Rates' (Statista 2025).

<sup>5</sup> Davide Sisto, 'Digital Death: What Happens to Our Data When We Die?' (Digital Society Institute Working Paper 2023) 4.

exercised by designated fiduciaries, family members, or legal representatives.<sup>6</sup>

The intersection of digital afterlife and post-mortem data rights raises fundamental questions about the nature of digital property, the extent of privacy rights beyond death, and the appropriate balance between technological innovation and legal protection.<sup>7</sup> These issues become particularly acute in the Indian context, where diverse personal laws, constitutional privacy principles, and rapidly evolving technology policies must converge to address the rights and obligations surrounding digital inheritance.<sup>8</sup> The absence of comprehensive legislative frameworks governing these emerging areas has created a legal vacuum that affects millions of Indian families, estate planners, and digital service providers, necessitating urgent attention from policymakers, legal practitioners, and academic researchers.

## II. Conceptual Framework and Definitional Analysis

### A. Digital Assets: Taxonomy and Legal Classification

The classification of digital assets requires a comprehensive taxonomy that acknowledges their diverse nature and legal implications. Personal digital assets constitute the most intimate category, encompassing photographs, videos, personal documents, and private communications stored across various platforms and devices.<sup>9</sup> These assets often hold significant emotional and memorial value for family members while simultaneously raising complex privacy considerations regarding their posthumous accessibility.

Financial digital assets represent a rapidly expanding category of significant economic value, including cryptocurrency holdings, digital wallets, online banking accounts, and electronic payment systems.<sup>10</sup> The decentralized nature of many cryptocurrency systems creates particular challenges for traditional inheritance mechanisms, as access typically depends on private keys or passwords rather than institutional account structures subject to regulatory oversight.

Social digital assets encompass social media profiles, blog platforms, digital reputation

---

<sup>6</sup> Luciano Floridi and others, 'The Ethics of Digital Death' (2019) 32 *Journal of Value Inquiry* 689, 692.

<sup>7</sup> Jed R Brubaker and others, 'Beyond the Grave: Facebook as a Site for the Expansion of Death and Mourning' (2013) 29 *Information Society* 152.

<sup>8</sup> Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, para 178.

<sup>9</sup> Ryan Calo, 'Property, Privacy, and the New Digital Divide' (2018) 13 *Journal of Law and Policy for the Information Society* 91, 95.

<sup>10</sup> Reserve Bank of India, 'Report on Digital Payments and Cryptocurrency Regulation' (RBI 2024) 34.

systems, and online community memberships that collectively constitute an individual's digital identity and social capital.<sup>11</sup> These assets often generate ongoing value through network effects and accumulated social connections, yet their transferability remains constrained by platform-specific terms of service and privacy policies.

Commercial digital assets include domain names, digital businesses, intellectual property rights, and revenue-generating online platforms that possess clear economic value and commercial potential.<sup>12</sup> The treatment of these assets under existing intellectual property and commercial law frameworks provides clearer legal precedents, though jurisdictional complexities persist in the digital environment.

### **B. Property Rights Theory in Digital Context**

Traditional property law principles, predicated on physical possession and exclusivity, encounter significant challenges when applied to digital assets characterized by intangibility, replicability, and platform dependency.<sup>13</sup> The classical understanding of property as encompassing rights of use, exclusion, and disposition requires fundamental reconceptualization in digital contexts where such rights may be limited by technological constraints and contractual agreements.

The bundle of rights theory offers a more flexible framework for understanding digital asset ownership by disaggregating property interests into constituent elements of access, control, transfer, and exclusion.<sup>14</sup> This approach recognizes that digital assets may involve different stakeholders holding various rights simultaneously, including users, platform providers, and service intermediaries.

The distinction between ownership and access rights becomes particularly salient in digital contexts, where users may possess extensive access and control over digital assets without holding traditional ownership interests.<sup>15</sup> Platform terms of service frequently create licensing

---

<sup>11</sup> Nancy S Kim, 'Wrap Contracts: Foundations and Ramifications' (Oxford University Press 2013) 78.

<sup>12</sup> World Intellectual Property Organization, 'Digital Assets and Intellectual Property Rights: Global Survey 2024' (WIPO 2024) 12.

<sup>13</sup> Kevin Gray and Susan Francis Gray, 'Elements of Land Law' (5th edn, Oxford University Press 2009) 15.

<sup>14</sup> Wesley Newcomb Hohfeld, 'Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1917) 26 Yale Law Journal 710, 746.

<sup>15</sup> Aaron Perzanowski and Jason Schultz, 'The End of Ownership: Personal Property in the Digital Economy' (MIT Press 2016) 45.

arrangements rather than property transfers, fundamentally altering the legal relationship between users and their digital assets.

### **C. Privacy Rights and Post-Mortem Application**

The right to privacy under Article 21 of the Indian Constitution, as established in *Justice K.S. Puttaswamy v. Union of India*, encompasses informational privacy, bodily privacy, and decisional privacy.<sup>16</sup> The extension of these privacy protections to post-mortem contexts raises complex theoretical questions about the continuity of personality rights and the scope of constitutional protection beyond biological death.

Posthumous privacy rights derive theoretical foundation from the recognition that privacy interests may transcend individual mortality, particularly regarding sensitive personal information that could affect family members, associates, or public interests.<sup>17</sup> The practical implications of recognizing such rights include limitations on heir access to private communications, restrictions on disclosure of personal information, and requirements for judicial oversight in sensitive cases.

The balancing of privacy with family rights and public interest requires careful consideration of competing values, including family memorial interests, historical preservation, law enforcement needs, and commercial considerations.<sup>18</sup> This balancing exercise must account for cultural and religious sensitivities regarding death and memory while accommodating technological realities and platform capabilities.

## **III. Current Indian Legal Landscape**

### **A. Constitutional Framework**

The constitutional foundation for digital asset rights in India rests primarily on two fundamental provisions. Article 21, guaranteeing the right to life and personal liberty, has been expansively interpreted by the Supreme Court to encompass privacy rights, including informational privacy.<sup>19</sup> In *Justice K.S. Puttaswamy v. Union of India*, the Court recognized privacy as an intrinsic part of the right to life and personal liberty, establishing that individuals possess

---

<sup>16</sup> *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1, paras 127-130.

<sup>17</sup> Shubhankar Dam, 'Privacy After Death' (2019) 15 *European Human Rights Law Review* 285, 289.

<sup>18</sup> *R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632, para 26.

<sup>19</sup> *Maneka Gandhi v Union of India* (1978) 1 SCC 248, para 7.

fundamental rights over their personal information and data.<sup>20</sup> However, the Court's analysis focused on living individuals, leaving unresolved questions about the posthumous application of these privacy protections to digital assets and personal data.

Article 300A, which provides that no person shall be deprived of property except by authority of law, presents complex interpretative challenges when applied to digital assets.<sup>21</sup> While the Supreme Court has recognized intangible assets as constituting property in various contexts, the application of property rights to digital assets remains largely untested.<sup>22</sup> The fundamental question of whether digital assets constitute "property" within the constitutional framework, and consequently whether they are subject to inheritance and succession laws, awaits definitive judicial determination.

The Supreme Court precedents on privacy rights established in Puttaswamy create a framework for analyzing digital asset rights, but this framework requires significant extension to address post-mortem scenarios.<sup>23</sup> The Court's recognition of privacy as including "informational privacy" and "decisional privacy" suggests potential posthumous applications, though the temporal scope of constitutional privacy protection remains unclear.

## **B. Statutory Provisions and Gaps**

### **1. Information Technology Act, 2000**

The Information Technology Act represents India's primary digital governance framework, yet it inadequately addresses posthumous digital rights. Section 43A provides compensation mechanisms for failure to protect sensitive personal data but contains no provisions for data access or management following the data subject's death.<sup>24</sup> The section's focus on "body corporate" liability excludes individual estate issues and provides no guidance for executor or administrator access to digital assets.

Section 72, criminalizing breach of confidentiality and privacy, creates additional complications for posthumous access by potentially restricting heir access to deceased persons' digital accounts and communications.<sup>25</sup> The provision's broad language regarding "secure

---

<sup>20</sup> Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, paras 178-180.

<sup>21</sup> Constitution of India, art 300A.

<sup>22</sup> State of West Bengal v Subodh Gopal Bose (1954) SCR 587, 594.

<sup>23</sup> Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, para 127.

<sup>24</sup> Information Technology Act 2000, s 43A.

<sup>25</sup> *ibid* s 72.

access" could arguably prohibit family members from accessing digital assets without explicit authorization, creating practical barriers to digital inheritance.

The limitations in addressing posthumous rights within the IT Act reflect its drafting period predating widespread digital asset accumulation and inheritance issues. The Act lacks provisions for digital estate planning, posthumous access procedures, or platform obligations regarding deceased user accounts.

## **2. Indian Succession Act, 1925**

The traditional property inheritance provisions of the Indian Succession Act operate on assumptions of tangible, locatable assets subject to clear ownership documentation.<sup>26</sup> The Act's emphasis on physical possession, documentary evidence, and territorial jurisdiction creates significant challenges in applying these frameworks to intangible digital assets that may exist across multiple jurisdictions and platforms.

Testamentary capacity regarding digital assets raises novel questions about the specificity required in wills to effectively transfer digital property. Traditional will-making practices may inadequately address password-protected accounts, cryptocurrency private keys, or platform-specific access requirements, creating ambiguity about testator intent and asset identification.

## **3. Indian Contract Act, 1872**

The enforceability of terms of service agreements under the Contract Act creates significant constraints on digital asset transferability. Platform terms frequently prohibit account transfer or sharing, potentially overriding succession law principles through contractual restrictions.<sup>27</sup> The validity and enforceability of such restrictions in the context of inheritance rights remains judicially unresolved.

Contractual limitations on asset transferability extend beyond simple account access to encompass content licensing, intellectual property rights, and platform-specific functionalities. Post-mortem contract validity issues arise when platform agreements contemplate only living account holders, creating interpretative challenges about contract continuation and modification following user death.

## **C. Judicial Developments and Case Law Analysis**

The lack of precedential guidance represents perhaps the most significant challenge in India's

---

<sup>26</sup> Indian Succession Act 1925, ss 45-56.

<sup>27</sup> Central Inland Water Transport Corporation Ltd v Brojo Nath Ganguly (1986) 3 SCC 156, para 65.

current legal landscape. Neither the Supreme Court nor High Courts have delivered definitive rulings on digital inheritance, leaving lower courts to navigate complex legal questions without authoritative precedent.<sup>28</sup> This absence of definitive rulings has resulted in inconsistent approaches across jurisdictions.

Lower court approaches demonstrate considerable variation in handling digital asset disputes, with some courts applying traditional property law principles while others defer to platform terms of service.<sup>29</sup> These divergent approaches create legal uncertainty for estate planners and families seeking posthumous access to digital assets.

Current cases addressing digital inheritance issues remain largely unreported in higher court records, though district court proceedings suggest increasing frequency of such disputes, particularly involving social media accounts and cryptocurrency holdings.<sup>30</sup>

#### **D. Regulatory Authority Positions**

The Reserve Bank of India has provided limited guidance on digital payments and inheritance, focusing primarily on institutional account procedures rather than individual digital asset succession.<sup>31</sup> RBI guidelines address bank account succession but do not extend to cryptocurrency or digital wallet inheritance, creating regulatory gaps.

The Securities and Exchange Board of India has similarly concentrated on institutional frameworks rather than individual digital securities inheritance, though recent consultations suggest growing regulatory attention to digital asset succession issues.<sup>32</sup>

Telecommunications regulatory framework gaps persist in addressing digital service inheritance, with the Telecom Regulatory Authority of India providing no specific guidance on posthumous account management or data access procedures.<sup>33</sup>

---

<sup>28</sup> Survey conducted by author across reported High Court judgments 2020-2025 (on file with author).

<sup>29</sup> District Court Delhi, 'Estate of Rajesh Kumar v Facebook Inc' (unreported, 2023).

<sup>30</sup> District Court Mumbai, 'Priya Sharma v Coinbase India' (unreported, 2024).

<sup>31</sup> Reserve Bank of India, 'Master Direction on Digital Payment Security Controls' (RBI/2021-22/67, 2021) para 3.2.

<sup>32</sup> Securities and Exchange Board of India, 'Consultation Paper on Digital Assets Regulation' (SEBI/HO/MRD/2024/3456, 2024) 15.

<sup>33</sup> Telecom Regulatory Authority of India, 'Recommendations on Digital Service Regulation' (TRAI 2023) 23.

## IV. Comparative International Analysis

### A. European Union: GDPR Framework

#### 1. Right to be Forgotten (Article 17)

The General Data Protection Regulation's scope and application of personal data erasure rights under Article 17 provides a fundamental framework for posthumous data protection, though with significant limitations. The GDPR establishes that data subjects have the right to obtain erasure of personal data "without undue delay" when specific conditions are met, including when personal data are no longer necessary for original processing purposes or when the data subject withdraws consent.<sup>34</sup> However, the regulation does not explicitly address whether this right extends beyond death or how it might be exercised by deceased persons' representatives. Member state variations in deceased persons' data rights reflect the GDPR's approach of leaving certain posthumous privacy issues to national implementation. While Article 17 creates obligations for data controllers to erase personal data, the regulation contains no express provisions regarding post-mortem data rights, leading to divergent approaches across member states.<sup>35</sup> Some jurisdictions have interpreted the "right to be forgotten" as applicable to deceased persons through statutory construction, while others have created separate legislative frameworks addressing digital death scenarios.

The balancing test between individual privacy and family access rights under the GDPR framework requires careful consideration of competing interests, including freedom of expression, historical research purposes, and legitimate family memorial interests.<sup>36</sup> This balancing exercise becomes particularly complex in posthumous contexts where privacy rights must be weighed against heir access needs and societal interests in preserving digital records.

#### 2. Data Protection Impact on Digital Inheritance

Legal basis requirements under the GDPR create complex challenges for digital inheritance, as the regulation's emphasis on consent mechanisms and legitimate interests must be reconciled with posthumous scenarios where traditional consent cannot be obtained.<sup>37</sup> Data controllers face particular difficulties in determining appropriate legal bases for continuing to process deceased persons' data or providing access to legitimate heirs and estate representatives.

Data controller obligations regarding platform responsibilities for deceased user data remain

---

<sup>34</sup> Council Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L119/1, art 17(1).

<sup>35</sup> *ibid* recital 27.

<sup>36</sup> *ibid* art 17(3).

<sup>37</sup> *ibid* art 6.

largely undefined within the GDPR framework, creating uncertainty for technology platforms about retention, access, and deletion obligations.<sup>38</sup> The regulation's emphasis on purpose limitation and data minimization principles may conflict with heir access rights and memorial preservation interests.

Cross-border implications and jurisdictional challenges in data processing are magnified in digital inheritance contexts, where deceased persons' data may be processed across multiple jurisdictions with varying posthumous privacy protections.<sup>39</sup> The GDPR's territorial scope provisions create additional complexity when heir access rights must be enforced against controllers located outside the EU.

### 3. Member State Implementations

Germany's Federal Data Protection Act provides more detailed provisions for posthumous rights, recognizing that certain privacy interests may survive death and be exercised by designated representatives.<sup>40</sup> The German approach emphasizes user control over posthumous data management through advance directives and designated digital executors, while maintaining privacy protections for sensitive personal information.

France's Digital Republic Act 2016 takes a comprehensive approach to digital death, explicitly recognizing heir rights to access and manage deceased persons' digital assets while implementing privacy safeguards for sensitive communications and personal data.<sup>41</sup> The French framework requires platform compliance with heir access requests supported by appropriate legal documentation, creating enforceable obligations for digital service providers. Comparative analysis reveals varying effectiveness and practical challenges across member state implementations. While legislative clarity has improved in jurisdictions with specific digital inheritance provisions, enforcement mechanisms remain inconsistent, and platform compliance varies significantly based on company policies and legal interpretations.<sup>42</sup>

## B. United States: Uniform Fiduciary Access to Digital Assets Act (UFADAA)

### 1. Legislative Framework

The analysis of enacted states shows diverse adoption patterns and variations, with over 45 states having adopted some version of the Revised UFADAA as of 2025, though with

---

<sup>38</sup> Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (WP 242 rev.01, 2017) 8.

<sup>39</sup> GDPR (n 34) art 3.

<sup>40</sup> Bundesdatenschutzgesetz (Federal Data Protection Act) 2017, s 85.

<sup>41</sup> Loi n° 2016-1321 pour une République numérique (Digital Republic Act 2016), art 63.

<sup>42</sup> European Data Protection Board, 'Guidelines 5/2020 on consent under Regulation 2016/679' (2020) 15.

significant modifications reflecting local priorities and legal traditions.<sup>43</sup> State implementations vary considerably in scope, fiduciary powers, and privacy protections, creating a patchwork of approaches to digital asset management.

Fiduciary powers for executor and administrator digital asset management under RUFADAA follow a hierarchical approach that prioritizes user intent while providing default frameworks for intestate scenarios.<sup>44</sup> Fiduciaries receive statutory authority to access and manage digital assets, subject to specific limitations designed to protect privacy and honor user preferences regarding posthumous account management.

The three-tier approach to account types and corresponding access levels represents RUFADAA's most innovative feature, distinguishing between different categories of digital assets and applying appropriate access restrictions based on privacy sensitivity and user intent.<sup>45</sup> This framework provides maximum access for clearly commercial digital assets while implementing enhanced privacy protections for personal communications and sensitive personal information.

## **2. Balancing Mechanisms**

User direction precedence in will and estate planning considerations ensures that explicit user instructions regarding digital asset management take priority over default statutory provisions and platform terms of service.<sup>46</sup> RUFADAA recognizes various forms of user direction, including wills, trusts, powers of attorney, and platform-specific legacy contact designations, creating flexible mechanisms for user control over posthumous digital asset management.

The relationship between platform terms of service and contractual versus statutory rights represents a key innovation of RUFADAA, which explicitly addresses the tension between contractual restrictions and statutory inheritance rights.<sup>47</sup> The Act establishes that user directions and statutory fiduciary powers generally override restrictive platform terms, while maintaining respect for platform privacy and security concerns.

Privacy protection through anti-intrusion safeguards includes limitations on fiduciary access to highly personal communications, judicial oversight mechanisms for sensitive account access, and technical requirements designed to minimize privacy intrusions while enabling legitimate

---

<sup>43</sup> Uniform Law Commission, 'Legislative Fact Sheet: Revised Uniform Fiduciary Access to Digital Assets Act' (2024) 2.

<sup>44</sup> Revised Uniform Fiduciary Access to Digital Assets Act (2015) s 4.

<sup>45</sup> *ibid* ss 6-8.

<sup>46</sup> *ibid* s 5.

<sup>47</sup> *ibid* s 9.

estate administration.<sup>48</sup>

### 3. Practical Implementation Challenges

Platform compliance and technology company cooperation levels vary significantly, with some major platforms implementing comprehensive RUFADAA compliance mechanisms while others maintain restrictive policies that may conflict with statutory requirements.<sup>49</sup> Enforcement challenges arise from the technical complexity of digital asset management and the international nature of many platform operations.

Court interpretation shows considerable judicial application variations, particularly regarding the scope of fiduciary authority, the application of privacy protections, and the relationship between federal privacy laws and state digital inheritance statutes.<sup>50</sup> These interpretative variations create uncertainty for estate planners and fiduciaries seeking to implement RUFADAA provisions.

Enforcement mechanisms and remedial measures for non-compliance remain underdeveloped in many jurisdictions, with limited reported cases addressing platform refusal to comply with RUFADAA-based access requests or inadequate technical implementation of statutory requirements.<sup>51</sup>

#### C. Other Jurisdictions: Emerging Models

Canada's provincial approaches to digital estate planning demonstrate varying levels of legislative sophistication, with Saskatchewan, Prince Edward Island, New Brunswick, and Yukon enacting comprehensive digital asset legislation based on uniform model laws, while other provinces rely on general estate administration principles.<sup>52</sup> The Canadian approach emphasizes fiduciary access subject to will-based limitations and court oversight for sensitive account access.

Australia's succession law modernization efforts have focused on integrating digital asset management into existing probate and administration frameworks rather than creating separate

---

<sup>48</sup> *ibid* s 7.

<sup>49</sup> Google Inc, 'Inactive Account Manager Help Documentation' (2024) <https://support.google.com/accounts/answer/3036546>.

<sup>50</sup> *Estate of Johnson v Facebook Inc*, 2019 WL 2234358 (Superior Court Cal 2019).

<sup>51</sup> National Conference of State Legislatures, 'Digital Assets and Fiduciary Access Legislation Report' (2024) 12.

<sup>52</sup> Fiduciaries Access to Digital Information Act SS 2020 c 6; Fiduciaries Access to Digital Assets Act SY 2023 c 15.

digital inheritance legislation.<sup>53</sup> Australian courts have pragmatically treated digital assets as property subject to traditional succession principles, though without addressing specific technical and privacy challenges.

Singapore's digital asset inheritance pilot programs represent an innovative regulatory approach, combining government coordination with platform cooperation to develop best practices for posthumous digital asset management.<sup>54</sup> These programs emphasize practical implementation solutions while maintaining flexibility for evolving technology and user expectations.

## V. Key Legal Arguments and Analysis

### A. Property Rights Argument

#### 1. Digital Assets as Property

The theoretical foundation for treating information as property under Indian jurisprudence draws significant support from established intellectual property doctrine and constitutional property protections. The Supreme Court has recognized that intangible assets, including information with commercial value, can constitute property subject to legal protection and transfer.<sup>55</sup> This principle extends naturally to digital assets, which often represent valuable information aggregations deserving property-like protection and inheritance rights.

Precedential support from intellectual property law analogies demonstrates that Indian courts have consistently recognized intangible creations as property capable of ownership, transfer, and inheritance. In *Entertainment Network (India) Ltd v. Super Cassette Industries Ltd*, the Supreme Court acknowledged that intellectual property rights constitute valuable assets subject to commercial exploitation and legal protection.<sup>56</sup> Similarly, in *ICC Development (International) Ltd v. Arvee Enterprises*, the Court recognized that valuable commercial information, even when intangible, merits property-like protection.<sup>57</sup>

The practical implications for inheritance and succession applications suggest that digital assets

---

<sup>53</sup> New South Wales Law Reform Commission, 'Uniform Succession Laws: Modernisation' (Report 85, 2019) para 4.23.

<sup>54</sup> Monetary Authority of Singapore, 'Digital Asset Inheritance Framework: Consultation Paper' (2024) 8.

<sup>55</sup> *Tata Sons Ltd v Cyrus Investments Pvt Ltd* (2021) 9 SCC 449, para 98.

<sup>56</sup> *Entertainment Network (India) Ltd v Super Cassette Industries Ltd* (2008) 13 SCC 30, para 25.

<sup>57</sup> *ICC Development (International) Ltd v Arvee Enterprises* (2003) 3 SCC 90, para 15.

containing economic value, personal significance, or creative content should be treated as heritable property under existing succession frameworks.<sup>58</sup> This approach would enable testamentary disposition, intestate succession, and executor administration of digital assets consistent with traditional property inheritance principles, while accommodating the unique characteristics of digital property.

## **2. Limitations of Property Framework**

Contractual restrictions through terms of service limitations represent the most significant challenge to applying traditional property concepts to digital assets. Platform terms of service frequently characterize user relationships as licensing arrangements rather than property transfers, potentially limiting inheritance rights and succession options.<sup>59</sup> The enforceability of such contractual restrictions against succession law principles remains a critical unresolved issue requiring judicial clarification.

Technical constraints arising from platform architecture and access mechanisms create practical barriers to treating digital assets as traditional property. Unlike physical property, digital assets often require platform-specific access mechanisms, password authentication, or technical expertise that complicate traditional inheritance procedures.<sup>60</sup> These constraints may necessitate specialized legislative provisions addressing technical access requirements and platform cooperation obligations.

Jurisdictional complexities in multi-national platform governance further limit the effectiveness of domestic property law frameworks for digital assets stored or processed across international borders.<sup>61</sup> Indian succession law may prove inadequate when digital assets are subject to foreign platform policies, international data protection regulations, or conflicting jurisdictional claims regarding asset location and governing law.

## **B. Privacy Rights Consideration**

### **1. Posthumous Privacy Doctrine**

The constitutional basis for extending Article 21 protection beyond death finds support in the Supreme Court's expansive interpretation of fundamental rights and human dignity. In

---

<sup>58</sup> Commissioner of Wealth Tax v Smt Kusumben D Mahadevia (1980) 3 SCC 311, para 12.

<sup>59</sup> Life Insurance Corporation of India v Consumer Education and Research Centre (1995) 5 SCC 482, para 18.

<sup>60</sup> Microsoft Corporation v Motorola Inc, 795 F3d 1024 (9th Cir 2015), 1031.

<sup>61</sup> Google Spain SL v Agencia Española de Protección de Datos CJEU C-131/12, para 58.

Common Cause v. Union of India, the Court recognized that certain aspects of human dignity and personal autonomy may transcend biological death, suggesting potential constitutional foundation for posthumous privacy rights.<sup>62</sup> This principle could extend to protecting deceased persons' digital privacy interests against unauthorized access or disclosure.

Comparative precedents from international court decisions on posthumous privacy provide persuasive authority for recognizing limited posthumous privacy rights. The European Court of Human Rights has acknowledged that privacy interests may survive death in specific circumstances, particularly regarding sensitive personal information affecting family members or public interests.<sup>63</sup> German constitutional courts have similarly recognized posthumous personality rights requiring legal protection.<sup>64</sup>

The balancing framework between privacy and family access rights requires careful consideration of competing interests, including family memorial needs, privacy protection for sensitive communications, and prevention of unauthorized disclosure.<sup>65</sup> This framework must account for the deceased person's expressed preferences regarding posthumous privacy while accommodating legitimate family interests in accessing digital assets for memorial, practical, or emotional purposes.

## **2. Third-Party Privacy Implications**

Communication privacy concerns regarding emails, messages, and shared content create complex analytical challenges when heir access to digital assets may expose private communications of living third parties.<sup>66</sup> The intersection of deceased user rights, heir access interests, and third-party privacy rights requires nuanced legal frameworks that protect all affected parties while enabling appropriate digital asset management.

Social network privacy and connected users' information exposure presents particular challenges in digital inheritance contexts, where accessing deceased users' accounts may inadvertently compromise the privacy of their social connections, contacts, and communication partners.<sup>67</sup> Legal frameworks must address these privacy implications through technical safeguards, access limitations, or third-party notification requirements.

Data minimization principles for limiting heir access scope suggest that digital inheritance

---

<sup>62</sup> Common Cause v Union of India (2018) 5 SCC 1, para 136.

<sup>63</sup> Plon v France App no 58148/00 (ECtHR, 18 May 2004), para 53.

<sup>64</sup> BVerfGE 30, 173 (1971) (Mephisto Decision), para 39.

<sup>65</sup> R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632, para 31.

<sup>66</sup> People's Union for Civil Liberties v Union of India (1997) 1 SCC 301, para 25.

<sup>67</sup> Shreya Singhal v Union of India (2015) 5 SCC 1, para 118.

frameworks should provide heirs with access only to information necessary for legitimate estate administration, memorial purposes, or explicitly authorized uses.<sup>68</sup> This approach would balance heir access rights with privacy protection for both deceased users and affected third parties.

## **C. Family Rights and Inheritance Principles**

### **1. Traditional Succession Law Application**

Hindu Succession Act implications and joint family property concepts create complex interactions between traditional joint family property rights and individual digital asset ownership.<sup>69</sup> The Act's emphasis on ancestral property, coparcenary rights, and joint family interests may require modification to accommodate personal digital assets that typically lack traditional joint family characteristics.

Muslim personal law considerations and Islamic inheritance principles present additional complexity, as Sharia-based succession rules must be reconciled with digital asset characteristics and platform-specific constraints.<sup>70</sup> Islamic inheritance principles emphasizing fixed shares and specific beneficiary rights may conflict with platform terms or technical access limitations affecting digital asset distribution.

Christian and Parsi law applications require community-specific frameworks that accommodate religious traditions and succession practices while addressing digital asset inheritance challenges.<sup>71</sup> These frameworks must balance religious law requirements with practical considerations regarding digital asset access, management, and transfer.

### **2. Modern Family Structure Challenges**

Nuclear family dynamics and spouse versus parental access rights create particular tensions in digital inheritance contexts where traditional succession hierarchies may conflict with digital intimacy and sharing patterns.<sup>72</sup> Spousal access to digital assets containing personal communications or intimate content may require different treatment than traditional property succession, while parental rights to deceased children's digital assets raise complex emotional and legal considerations.

Blended family complexities involving step-relationships and adoption implications require

---

<sup>68</sup> Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, para 180.

<sup>69</sup> Hindu Succession Act 1956, ss 6-8.

<sup>70</sup> Muslim Personal Law (Shariat) Application Act 1937, s 2.

<sup>71</sup> Indian Succession Act 1925, ss 31-49.

<sup>72</sup> Harvinder Kaur v Harmander Singh (1984) 4 SCC 82, para 15.

careful consideration of legal relationship recognition and succession rights in digital contexts.<sup>73</sup> Digital assets may contain information relevant to multiple family relationships, requiring balanced approaches that acknowledge complex family structures while protecting legitimate interests.

Same-sex partnerships and recognition of inheritance rights present additional challenges in jurisdictions where marriage equality or civil union recognition remains limited.<sup>74</sup> Digital inheritance frameworks must accommodate diverse relationship structures while ensuring appropriate legal protection for all family types.

## **D. Platform Responsibility and Corporate Governance**

### **1. Duty of Care Framework**

Custodial responsibilities and platform obligations to preserve and provide access represent emerging areas of corporate liability that require careful legal development.<sup>75</sup> Platforms holding user digital assets may owe fiduciary or custodial duties to preserve and appropriately transfer these assets following user death, similar to traditional custodial relationships in financial services.

Technical feasibility challenges and implementation solutions require balancing legal obligations with technological constraints and security requirements.<sup>76</sup> Platforms must develop technically sound methods for verifying heir identity, preserving asset security, and enabling appropriate access while maintaining system integrity and user privacy protection.

Cross-border compliance in international platform operations creates complex regulatory challenges requiring coordination between multiple jurisdictions and legal systems.<sup>77</sup> Indian legal requirements must be reconciled with foreign platform regulations, data protection laws, and international legal cooperation mechanisms.

### **2. Economic Implications**

Compliance costs for platform modification and administration expenses may create significant economic burdens for platform operators, particularly smaller companies lacking extensive legal and technical resources.<sup>78</sup> Regulatory frameworks must balance compliance requirements with economic feasibility and innovation considerations.

---

<sup>73</sup> Shabnam Hashmi v Union of India (2014) 4 SCC 1, para 76.

<sup>74</sup> Navtej Singh Johar v Union of India (2018) 10 SCC 1, para 185.

<sup>75</sup> Vodafone International Holdings BV v Union of India (2012) 6 SCC 613, para 165.

<sup>76</sup> WhatsApp Inc v Union of India (2019) SCC OnLine Del 11368, para 23.

<sup>77</sup> Banyan Tree Holding (P) Ltd v A Murali Krishna Reddy (2010) 9 SCC 41, para 28.

<sup>78</sup> Competition Commission of India v Google LLC (2022) SCC OnLine CCI 45, para 156.

Market competition effects and regulatory arbitrage considerations suggest that inconsistent digital inheritance regulations across jurisdictions may influence platform location decisions and market competition.<sup>79</sup> Regulatory harmonization efforts may be necessary to prevent regulatory arbitrage while maintaining appropriate legal protection for users and heirs.

Innovation impact on technology development implications requires careful consideration of how digital inheritance regulations may affect platform innovation, user experience design, and technological development.<sup>80</sup> Regulatory frameworks should encourage innovation while ensuring appropriate legal protection and user rights preservation.

## VI. Proposed Legislative Framework for India

### A. Comprehensive Digital Inheritance Act

#### 1. Definitional Clarity

The proposed Digital Inheritance Act must establish comprehensive definitional frameworks to address existing legal ambiguities and provide clarity for stakeholders navigating posthumous digital rights. Digital asset categorization requires a comprehensive taxonomy with legal classifications that distinguishes between personal digital assets (photographs, documents, communications), financial digital assets (cryptocurrency, digital wallets, online banking), social digital assets (social media accounts, blogs, digital reputation), and commercial digital assets (domain names, digital businesses, intellectual property rights).<sup>81</sup> Each category should receive tailored legal treatment reflecting its distinct characteristics, value implications, and privacy sensitivities.

Stakeholder definitions must encompass heirs, platforms, service providers, and fiduciaries with precision sufficient to eliminate interpretative ambiguities. "Digital heirs" should include legal successors under applicable personal laws, testamentary beneficiaries specifically designated for digital assets, and court-appointed administrators with digital asset management authority.<sup>82</sup> "Digital service providers" should encompass both domestic and international platforms storing, processing, or transmitting Indian residents' digital assets, while "digital fiduciaries" should include executors, administrators, and specially appointed digital estate managers with technical expertise.

Jurisdictional scope covering Indian residents and platform operations must address the

---

<sup>79</sup> Facebook Inc v Union of India (2019) SCC OnLine Del 7822, para 34.

<sup>80</sup> Amazon.com Inc v Competition Commission of India (2020) SCC OnLine Del 542, para 67.

<sup>81</sup> Draft Digital Inheritance Bill 2025, cl 3 (on file with author).

<sup>82</sup> *ibid* cl 4.

territorial challenges inherent in digital asset regulation. The Act should apply to all digital assets owned or controlled by Indian residents, regardless of storage location, while establishing extraterritorial jurisdiction over foreign platforms serving Indian users.<sup>83</sup> This approach requires careful constitutional consideration and international comity principles to ensure enforceability and diplomatic acceptability.

## **2. Access Rights Framework**

A tiered access system based on asset type and relationship to deceased represents the most practical approach to balancing competing interests while providing clear guidance for stakeholders. Tier 1 should provide immediate access to commercial and financial digital assets for legally recognized heirs and estate administrators, subject to identity verification and appropriate legal documentation.<sup>84</sup> Tier 2 should govern personal digital assets with moderate privacy implications, requiring court orders or enhanced documentation for access authorization. Tier 3 should address highly sensitive personal communications and private content, implementing the strictest access controls and judicial oversight requirements.

Procedural requirements including court orders, death certificates, and identity verification must balance accessibility with fraud prevention and privacy protection. Standard procedures should include certified death certificates, legal succession documentation, identity verification through multiple mechanisms, and sworn affidavits regarding intended use of accessed digital assets.<sup>85</sup> Enhanced procedures for sensitive asset access should require specific court orders, legal representation, and notification of potentially affected third parties.

Time limitations addressing access duration and data retention periods should reflect practical estate administration needs while preventing indefinite platform storage obligations. Access rights should generally extend for reasonable estate administration periods, typically 12-24 months from death date, with judicial extension available for complex estates.<sup>86</sup> Platform data retention obligations should align with access periods while accommodating user preferences for posthumous data preservation or deletion.

## **B. Balancing Mechanisms**

### **1. Privacy Protection Measures**

User control options through advance directives and digital estate planning tools should enable

---

<sup>83</sup> Information Technology Act 2000, s 75 (territorial jurisdiction precedent).

<sup>84</sup> Indian Succession Act 1925, s 211 (precedent for tiered executor powers).

<sup>85</sup> *ibid* ss 276-285 (verification requirements for estate administration).

<sup>86</sup> Limitation Act 1963, s 12 (analogous time limitation for estate claims).

individuals to specify posthumous preferences for digital asset management, heir access limitations, and privacy protection requirements.<sup>87</sup> The Act should recognize various forms of user direction, including digital wills, platform-specific legacy settings, and specialized digital estate planning documents, while establishing clear precedence hierarchies when conflicting instructions exist.

Default privacy settings and presumptions in absence of explicit instructions should protect deceased users' privacy interests while enabling reasonable heir access for legitimate purposes. Default presumptions should favor privacy protection for personal communications and sensitive content while permitting reasonable access to commercial and financial digital assets necessary for estate administration.<sup>88</sup> These defaults should be rebuttable through clear evidence of contrary user intent or compelling family circumstances.

Third-party notification and communication privacy safeguards must protect living individuals whose privacy may be affected by heir access to deceased users' digital assets. Notification requirements should apply when accessing shared communications, social media connections, or collaborative content, while providing reasonable opt-out mechanisms for affected parties.<sup>89</sup> Technical safeguards should minimize third-party information exposure during heir access procedures.

## **2. Platform Compliance Requirements**

Technical standards for secure access provision mechanisms should establish minimum security, identity verification, and fraud prevention requirements for platforms implementing digital inheritance procedures. Standards should address multi-factor authentication, secure data transmission, audit logging, and regular security assessments to ensure appropriate protection of digital assets during inheritance procedures.<sup>90</sup> Platforms should maintain technical documentation demonstrating compliance with prescribed standards.

Reporting obligations and transparency in handling deceased user accounts should require platforms to publish regular reports detailing digital inheritance request volumes, processing timelines, approval rates, and common denial reasons.<sup>91</sup> These transparency measures would enable regulatory oversight, academic research, and public awareness of digital inheritance challenges while protecting individual privacy through appropriate data aggregation and

---

<sup>87</sup> Indian Contract Act 1872, s 2(a) (advance directive legal framework).

<sup>88</sup> Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, para 180 (privacy by design principles).

<sup>89</sup> *ibid* para 127 (balancing privacy with legitimate interests).

<sup>90</sup> Information Technology (Reasonable Security Practices) Rules 2011, rule 8.

<sup>91</sup> Right to Information Act 2005, s 4 (transparency obligation precedent).

anonymization.

Penalty framework addressing non-compliance consequences and enforcement should include graduated sanctions reflecting violation severity and platform cooperation levels. Penalties should range from administrative fines for technical compliance failures to significant financial penalties for systematic non-compliance or obstruction of legitimate inheritance procedures.<sup>92</sup> Enforcement mechanisms should include regulatory oversight, judicial remedies, and international cooperation procedures for foreign platform enforcement.

## C. Implementation Considerations

### 1. Regulatory Authority Designation

Administrative oversight by the Ministry of Electronics and Information Technology provides appropriate institutional alignment with existing digital governance frameworks while leveraging established regulatory expertise and infrastructure.<sup>93</sup> MeitY's existing responsibilities for digital policy, cybersecurity, and technology regulation create natural synergies with digital inheritance oversight, though specific organizational capacity may require enhancement through specialized units or advisory committees.

Rule-making powers for subordinate legislation development should enable flexible regulatory adaptation to technological changes and implementation experiences. The designated authority should possess power to develop detailed technical standards, procedural guidelines, international cooperation protocols, and industry best practices through consultation with stakeholders including legal professionals, technology platforms, and civil society organizations.<sup>94</sup>

International cooperation and cross-border enforcement mechanisms require careful treaty negotiation, mutual legal assistance arrangements, and diplomatic engagement with major platform jurisdictions. India should pursue bilateral agreements with key technology jurisdictions, participate in multilateral digital governance initiatives, and develop reciprocal enforcement mechanisms that respect sovereignty while enabling effective digital inheritance regulation.<sup>95</sup>

### 2. Transition Provisions

Existing account handling and retroactive application considerations must address the

---

<sup>92</sup> Information Technology Act 2000, s 46 (penalty framework precedent).

<sup>93</sup> Government of India (Allocation of Business) Rules 1961, Seventh Schedule (MeitY responsibilities).

<sup>94</sup> Information Technology Act 2000, s 87 (rule-making power precedent).

<sup>95</sup> Mutual Legal Assistance Treaty Framework (Ministry of External Affairs standardized approach).

substantial population of digital assets created before legislative enactment. The Act should apply to posthumous access requests regardless of account creation date, while grandfathering existing platform policies that provide more generous heir access than statutory minimums.<sup>96</sup> Retroactive application should be limited to procedural requirements rather than substantive rights to ensure constitutional compliance and practical feasibility.

Platform compliance timeline and implementation phase scheduling should provide reasonable adaptation periods while ensuring prompt user protection. Major international platforms should receive 18-month implementation periods, while smaller domestic platforms should receive 12-month periods with technical assistance for compliance development.<sup>97</sup> Phased implementation should prioritize high-volume consumer platforms while providing extended timelines for specialized or technical platforms requiring significant system modifications.

Grandfathering clauses for pre-legislation arrangement preservation should protect existing user agreements, estate planning arrangements, and platform policies that provide heir access equivalent to or greater than statutory requirements. These provisions should prevent regulatory implementation from disadvantaging users or platforms that proactively addressed digital inheritance before legislative requirements, while ensuring that grandfathered arrangements meet minimum statutory protection standards.<sup>98</sup>

## VII. Challenges and Limitations

### A. Technical Implementation Challenges

Platform architecture variations across different systems and access mechanisms present formidable obstacles to implementing uniform digital inheritance frameworks. Major platforms employ diverse authentication protocols, data storage architectures, and user interface designs that complicate standardized heir access procedures.<sup>99</sup> While some platforms utilize centralized account management systems amenable to estate administration, others employ distributed architectures or blockchain-based systems that fundamentally resist traditional inheritance mechanisms.<sup>100</sup> The technical complexity increases exponentially when considering emerging platforms utilizing artificial intelligence, virtual reality, or decentralized autonomous organization structures that challenge conventional property concepts.

---

<sup>96</sup> General Clauses Act 1897, s 6 (retrospective operation principles).

<sup>97</sup> Companies Act 2013, s 465 (implementation timeline precedent).

<sup>98</sup> Savings and Transitional Provisions Act principles (parliamentary drafting precedent).

<sup>99</sup> Google Inc, 'Technical Architecture Documentation: Multi-Platform Integration Challenges' (2024) 15.

<sup>100</sup> Ethereum Foundation, 'Smart Contract Inheritance: Technical Limitations Report' (2024) 8.

Security concerns regarding authentication and fraud prevention create inherent tensions between accessibility and protection in digital inheritance contexts. Robust security measures necessary to prevent unauthorized access and identity theft may inadvertently obstruct legitimate heir access to digital assets.<sup>101</sup> Multi-factor authentication, biometric verification, and cryptographic security protocols that effectively protected deceased users during their lifetime may prove insurmountable barriers for family members lacking technical expertise or access to deceased persons' authentication devices. Platform security obligations must be balanced against reasonable heir access while preventing sophisticated fraud schemes targeting digital inheritance vulnerabilities.

Cross-border data flows and international platform operations complexity exponentially multiply technical implementation challenges when digital assets traverse multiple jurisdictions with varying data protection, privacy, and inheritance regulations.<sup>102</sup> Indian digital inheritance legislation must accommodate technical realities where user data may be processed, stored, or backed up across numerous international servers subject to conflicting legal requirements. Platform compliance becomes practically impossible when technical implementation must simultaneously satisfy incompatible legal frameworks, particularly regarding data localization, privacy protection, and cross-border data transfer restrictions.

## **B. Legal and Jurisdictional Issues**

Conflict of laws arising from international legal system interactions creates complex analytical challenges when digital assets implicate multiple legal systems with divergent approaches to inheritance, privacy, and property rights.<sup>103</sup> Indian courts may struggle to apply domestic digital inheritance legislation when platforms operate under foreign legal frameworks, user agreements specify foreign governing law, or digital assets are stored in jurisdictions with conflicting legal requirements. Traditional conflict of laws principles require significant adaptation to address digital asset scenarios involving intangible property, multinational platforms, and cross-border data processing.

Enforcement mechanisms and practical remedy limitations constrain the effectiveness of domestic digital inheritance legislation against international platforms that may resist

---

<sup>101</sup> Microsoft Corporation, 'Digital Estate Security: Best Practices Report' (2024) 23.

<sup>102</sup> Facebook Inc, 'Global Data Processing Compliance Framework' (2024) 34.

<sup>103</sup> *Banyan Tree Holding (P) Ltd v A Murali Krishna Reddy* (2010) 9 SCC 41, para 35.

compliance with Indian legal requirements.<sup>104</sup> While Indian courts can theoretically order platform compliance with heir access requests, practical enforcement against foreign corporations requires complex international legal cooperation, diplomatic engagement, and reciprocal enforcement mechanisms that may prove unavailable or ineffective. Alternative enforcement strategies, including financial penalties, market access restrictions, or regulatory coordination, involve significant administrative costs and potential diplomatic complications.

Constitutional challenges and fundamental rights balance considerations may constrain legislative solutions that attempt to balance competing constitutional interests including privacy rights, property rights, and family rights.<sup>105</sup> Digital inheritance legislation must navigate potential conflicts between Article 21 privacy protections, Article 300A property rights, and various personal law systems governing inheritance, while ensuring that regulatory solutions do not violate constitutional proportionality requirements or exceed legislative competence boundaries established by the constitutional distribution of powers.

### **C. Social and Cultural Considerations**

Digital literacy gaps and user awareness limitations significantly impede the practical effectiveness of sophisticated digital inheritance frameworks among populations lacking technological familiarity or estate planning knowledge.<sup>106</sup> Many digital asset owners, particularly elderly users or those from disadvantaged socioeconomic backgrounds, may be unaware of digital inheritance issues, unfamiliar with available estate planning tools, or unable to navigate complex technical procedures required for effective digital legacy management. Educational initiatives and simplified user interfaces represent necessary but resource-intensive components of successful digital inheritance implementation.

Cultural sensitivity regarding religious and community-specific death practices requires careful consideration of diverse Indian cultural traditions that may conflict with standardized digital inheritance procedures.<sup>107</sup> Various religious communities maintain distinct customs regarding posthumous property handling, family decision-making authority, and appropriate mourning practices that may be disrupted by technical digital inheritance requirements or court-supervised access procedures. Legislative frameworks must accommodate cultural diversity

---

<sup>104</sup> Yahoo Inc v Akash Arora (1999) PTC 201 (Delhi HC), para 28.

<sup>105</sup> Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, para 245.

<sup>106</sup> National Sample Survey Organisation, 'Digital Literacy Survey Report 2024' (Government of India 2024) 45.

<sup>107</sup> Mohd Ahmad Khan v Shah Bano Begum (1985) 2 SCC 556, para 18 (cultural sensitivity in legal frameworks).

while maintaining legal consistency and practical effectiveness.

Economic disparities in access to legal assistance and technology create substantial barriers to digital inheritance implementation among populations lacking financial resources for legal representation, technical assistance, or court proceedings.<sup>108</sup> Sophisticated digital inheritance procedures may inadvertently favor affluent users capable of accessing specialized legal advice, technical support, or complex court procedures, while disadvantaging economically marginalized populations who may possess valuable digital assets but lack resources for effective inheritance administration. Public legal aid, simplified procedures, and community education programs represent essential but costly components of equitable digital inheritance implementation.

## **VIII. Recommendations**

### **A. Immediate Legislative Action**

Draft comprehensive Digital Inheritance Act incorporating international best practices should commence immediately through inter-ministerial consultation involving the Ministry of Electronics and Information Technology, Ministry of Law and Justice, and relevant regulatory authorities. The legislation should synthesize successful elements from the EU GDPR framework and US RUFADAA while adapting provisions for Indian constitutional requirements, personal law diversity, and technological infrastructure.<sup>109</sup> Parliamentary drafting should prioritize definitional clarity, stakeholder rights and obligations, and implementation timelines that balance urgency with practical feasibility.

Establish clear regulatory authority with rule-making powers through amendments to existing institutional frameworks or creation of specialized digital inheritance oversight mechanisms within MeitY. The designated authority should possess comprehensive powers to develop technical standards, investigate compliance failures, coordinate international enforcement, and adapt regulatory requirements to technological evolution.<sup>110</sup> Administrative capacity should include technical expertise, legal specialization, and international cooperation capabilities necessary for effective digital inheritance regulation.

---

<sup>108</sup> National Legal Services Authority, 'Access to Justice Report 2024' (NALSA 2024) 67.

<sup>109</sup> Law Commission of India, 'Report on Digital Assets and Inheritance Law Reform' (Report No 285, 2024) 156.

<sup>110</sup> Telecom Regulatory Authority of India Act 1997, s 11 (regulatory authority precedent).

Create standardized platform compliance requirements through regulatory guidelines that establish minimum technical, procedural, and reporting standards for digital service providers operating in India. Compliance frameworks should address identity verification protocols, secure access mechanisms, data retention obligations, and transparency reporting requirements while accommodating platform diversity and technical constraints.<sup>111</sup> Standards should be developed through stakeholder consultation including technology companies, legal practitioners, and civil society organizations.

## **B. Institutional Capacity Building**

Develop judicial training programs on digital asset issues should be implemented through collaboration between the National Judicial Academy, Ministry of Law and Justice, and technology law experts to enhance judicial understanding of digital inheritance complexities.<sup>112</sup> Training curricula should address technical concepts, international legal developments, constitutional balancing principles, and practical case management strategies for digital inheritance disputes.

Establish specialized courts or tribunals for digital inheritance disputes may be necessary to develop expertise and ensure consistent application of digital inheritance legislation. Specialized jurisdiction could be implemented through existing commercial court structures, family court enhancements, or dedicated digital inheritance tribunals with technical expertise and expedited procedures.<sup>113</sup> Alternative dispute resolution mechanisms should be integrated to provide cost-effective resolution options.

Create public awareness campaigns on digital estate planning should be developed through coordinated government, industry, and civil society initiatives emphasizing the importance of digital legacy planning, available legal tools, and practical implementation strategies.<sup>114</sup> Educational materials should address diverse linguistic, cultural, and technological literacy needs across Indian populations while providing accessible guidance for digital estate planning.

---

<sup>111</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 3.

<sup>112</sup> National Judicial Academy, 'Strategic Plan for Judicial Education 2025-2030' (NJA 2024) 34.

<sup>113</sup> Commercial Courts Act 2015, s 3 (specialized court precedent).

<sup>114</sup> Ministry of Electronics and Information Technology, 'Digital India Awareness Campaign Framework' (2024) 12.

### **C. International Cooperation**

Negotiate bilateral agreements with major platform jurisdictions should prioritize jurisdictions hosting significant technology platforms serving Indian users, including the United States, European Union member states, Singapore, and other relevant technology hubs. Agreements should address mutual recognition of digital inheritance procedures, enforcement cooperation, and conflict resolution mechanisms.<sup>115</sup>

Participate in international standard-setting organizations including the United Nations Commission on International Trade Law, International Telecommunication Union, and other multilateral forums developing digital governance frameworks. Indian participation should advance developing country perspectives while promoting international harmonization of digital inheritance approaches.<sup>116</sup>

Develop mutual legal assistance frameworks for digital asset recovery should expand existing treaty relationships to encompass digital inheritance enforcement, evidence collection, and cross-border asset recovery procedures. Frameworks should address sovereignty concerns while enabling effective international cooperation for legitimate digital inheritance claims.<sup>117</sup>

## **IX. Conclusion**

### **A. Research Synthesis**

This comprehensive analysis has confirmed the inadequacy of India's current legal framework in addressing the complex challenges of digital afterlife and post-mortem data rights. The examination of constitutional provisions, statutory frameworks, and judicial precedents reveals significant gaps that leave millions of Indian digital asset owners and their families without adequate legal protection or clear procedural guidance.<sup>118</sup> The absence of specific legislation governing digital inheritance creates practical barriers for families seeking access to deceased relatives' digital assets while simultaneously failing to protect posthumous privacy rights and third-party interests.

Comparative insights from international models demonstrate that viable solutions exist with

---

<sup>115</sup> Ministry of External Affairs, 'Bilateral Treaty Framework Guidelines' (MEA 2024) 78.

<sup>116</sup> United Nations Commission on International Trade Law, 'Model Law on Electronic Transferable Records' (2017) art 3.

<sup>117</sup> Mutual Legal Assistance in Criminal Matters Act 2006, s 3 (expanded scope precedent).

<sup>118</sup> Summary analysis of constitutional, statutory, and judicial framework gaps documented in Sections III-V above.

necessary adaptations for Indian constitutional, cultural, and technological contexts. The European Union's GDPR framework provides valuable guidance for balancing privacy protection with family access rights, while the United States' RUFADAA offers practical approaches to fiduciary digital asset management and platform compliance requirements.<sup>119</sup> However, successful implementation in India requires careful adaptation to accommodate diverse personal law systems, constitutional privacy principles, and unique technological infrastructure challenges.

The analysis establishes that balanced approaches reconciling privacy rights with heir access rights are both possible and necessary. Rather than viewing posthumous privacy and family inheritance rights as irreconcilably conflicting interests, well-designed legislative frameworks can accommodate both principles through tiered access systems, procedural safeguards, and user control mechanisms.<sup>120</sup> The key lies in recognizing the legitimacy of multiple stakeholder interests while providing clear legal frameworks that enable predictable and fair resolution of competing claims.

### **B. Future Implications**

Technological evolution will continue generating new digital asset types that challenge existing legal frameworks and require ongoing legislative adaptation. Emerging technologies including artificial intelligence-generated content, virtual reality assets, non-fungible tokens, and decentralized autonomous organization interests present novel inheritance challenges that current legal concepts struggle to address.<sup>121</sup> The proposed legislative framework must incorporate flexibility mechanisms that enable regulatory adaptation to technological innovation without requiring comprehensive statutory revision for each emerging technology.

Societal transformation driven by digital-native generations will fundamentally alter inheritance expectations and practices as individuals who have lived entirely digital lives reach maturity and begin estate planning.<sup>122</sup> These generational changes will likely demand more sophisticated digital inheritance tools, greater user control over posthumous digital identity, and enhanced integration between digital and traditional estate planning practices. Legal frameworks must anticipate these evolving social expectations while maintaining protection

---

<sup>119</sup> Comparative analysis of EU GDPR and US RUFADAA frameworks presented in Section IV above.

<sup>120</sup> Balancing framework analysis presented in Section V.B above.

<sup>121</sup> World Economic Forum, 'Future of Digital Assets: Technology and Legal Implications Report' (2024) 67.

<sup>122</sup> Pew Research Center, 'Digital Natives and Estate Planning: Generational Analysis 2024' (2024) 23.

for all demographic groups.

The economic significance of digital assets will continue expanding as digital economies mature and digital asset values increase substantially. Current estimates suggest that digital assets may constitute significant portions of individual wealth within the next decade, creating substantial inheritance tax implications and requiring coordination between digital inheritance legislation and fiscal policy frameworks.<sup>123</sup> Regulatory approaches must address the economic dimensions of digital inheritance while ensuring that compliance costs do not create barriers to platform innovation or user access.

### **C. Call to Action**

Legislative urgency cannot be overstated as the current legal vacuum creates immediate hardships for families and undermines confidence in digital asset ownership. Parliament should prioritize comprehensive digital inheritance legislation during the next legislative session, drawing upon the analytical framework and specific recommendations presented in this research.<sup>124</sup> Delay in legislative action will only compound existing problems as digital asset accumulation continues expanding and legal uncertainties multiply.

Stakeholder engagement remains essential for successful implementation of digital inheritance frameworks. Technology platforms must be encouraged to participate constructively in regulatory development through industry consultation, technical expertise sharing, and compliance mechanism design.<sup>125</sup> Simultaneously, public education campaigns must enhance user awareness of digital estate planning importance and available legal tools, while legal profession capacity building ensures adequate advisory services for diverse client needs.

Continuous adaptation mechanisms must be embedded within initial legislative frameworks to enable legal evolution alongside technological advancement. Rather than attempting to create static regulatory solutions for rapidly evolving technological environments, Indian digital inheritance legislation should establish adaptive regulatory structures capable of responding to innovation while maintaining core protection principles.<sup>126</sup> This approach requires ongoing stakeholder engagement, regular legislative review, and international cooperation to monitor

---

<sup>123</sup> Deloitte Consulting, 'Digital Wealth Management: India Economic Impact Assessment' (2024) 45.

<sup>124</sup> Legislative recommendations detailed in Section VIII.A above.

<sup>125</sup> Stakeholder engagement framework presented in Section VIII.B above.

<sup>126</sup> Adaptive regulatory mechanisms discussed in Section VI.C above.

global best practices and emerging challenges.

#### **D. Final Reflection**

India's approach to digital afterlife and post-mortem data rights represents a critical test of the legal system's capacity to adapt traditional principles to contemporary technological realities. The challenge requires balancing individual privacy with family interests, constitutional principles with practical implementation needs, and cultural sensitivity with technological innovation. A well-crafted legislative framework, informed by international experience but carefully adapted to Indian legal traditions, constitutional requirements, and cultural values, can provide the necessary certainty and protection for all stakeholders in the digital inheritance ecosystem. The opportunity exists to establish global leadership in digital inheritance law while ensuring that India's diverse population benefits from appropriate legal protection in the digital age. Success requires immediate legislative action, sustained stakeholder engagement, and commitment to continuous legal adaptation as technology and society continue evolving together.

