INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL AFTERLIFE AND CYBER CRIME: WHO OWNS AND CONTROLS DATA AFTER DEATH?

AUTHORED BY - NABYAA NIYATI
Semester: 8th
Stream: B.A.LL.B. (Hons.), KIIT School of Law

I. Abstract

The widespread adoption of digital technologies has fundamentally altered the nature of human existence, extending individual identity beyond the limitations of physical life into a persistent virtual realm. This paper investigates the nascent concept of the digital afterlife, defined as the continued existence and possible application of a deceased person's digital information. With the rise of social media networks, cloud-based services, financial platforms, and many other online spaces, people now leave behind a lot of electronic footprints that raise complicated legal, ethical, and regulatory questions. The study critically analyzes the deficiencies of India's current legal framework in addressing issues related to posthumous digital data. The Information Technology Act of 2000 and the Indian Succession Act of 1925 do not give clear answers to questions about who owns, inherits, and controls digital assets after someone dies. Additionally, the Digital Personal Data Protection Act, 2023 does not clearly extend its protections to include privacy after death, which means that data belonging to deceased people is not well protected. The paper also looks into the rise in cyber crimes that involve the illegal use of dead people's digital identities, such as identity theft, financial fraud, and pretending to be someone else on social media. It highlights the challenges of incorporating such behavior into current statutory frameworks and the evidentiary issues stemming from the absence of established methods for authentication and legal representation. A comparative analysis of international frameworks, including the Revised Uniform Fiduciary Access to Digital Assets Act of the United States and the General Data Protection Regulation of the European Union, reveals a fragmented and inconsistent global response, marked by varying degrees of recognition granted to digital inheritance and posthumous rights. The study delineates several critical legal and ethical issues, including the conflict between proprietary claims and personality rights, the difficulty of determining valid consent in the absence of the data subject, and the increasing power of private corporations like Google LLC and Meta Platforms in

ISSN: 2582-6433

influencing digital legacies through their contractual agreements. The paper asserts that a balanced methodology is necessary, one that reconciles property-centric interests with the respect and independence due to the deceased. To address these issues, the paper proposes a thorough reform agenda that includes the creation of specific laws about digital inheritance, the formal recognition of posthumous data rights, the introduction of legally recognized digital executors, and the alignment of platform-specific policies with national laws. It also stresses how important it is to strengthen laws against cyber crime and raise awareness of digital estate planning. The paper concludes that, in the absence of prompt legislative intervention, the risks associated with the digital afterlife will persistently escalate. It emphasizes the necessity for the law to adapt to these advancements, safeguarding the dignity of individuals in the digital realm posthumously.

Keywords: Digital Afterlife, Digital Inheritance, Posthumous Privacy, Cyber Crime, Digital Assets, Succession Law, Data Protection, Identity Theft, Platform Governance, Digital Executor.

II. Introduction

In this age of widespread digital connectivity, human existence transcends the physical realm and significantly encompasses virtual space. The idea of a digital afterlife refers to the fact that a person's digital data can still be accessed, used, and stored even after they die. This kind of data includes social media profiles, emails, files stored in the cloud, online bank accounts, and other electronic traces that make up a person's online identity.

As digital platforms grow at an exponential rate, people collect huge amounts of personal data over the course of their lives. As the number of digital assets continues to grow, there are more and more legal and moral questions about what happens to this data after someone dies. Unlike traditional forms of property, digital data is often governed by contracts with service providers, such as terms of service and privacy policies, which seldom include sufficient clauses concerning succession or posthumous control.

There is a lot of legal confusion about who owns and controls digital assets after the person who made them dies. Without explicit statutory provisions, it is ambiguous whether such data forms part of the deceased's estate, whether legal heirs have the right to inherit it, or whether its control remains with the service provider. This uncertainty is exacerbated by the increasing

ISSN: 2582-6433

prevalence of cybercrimes involving the misappropriation of deceased individuals' data, particularly through identity theft, financial fraud, and unauthorized account access.

In light of this context, the current research aims to achieve three primary objectives: firstly, to examine the current legal framework and pinpoint its deficiencies in governing digital assets post-mortem; secondly, to evaluate the cyber threats linked to the improper use of posthumous data; and thirdly, to recommend legal and policy measures that would enhance clarity, protect rights, and ensure accountability in this evolving legal domain.

The investigation is consequently centered on the question: Who possesses legitimate ownership of digital data post-mortem? Can existing cyber laws be used to effectively prosecute people who misuse this kind of information? And does the Indian legal system have what it needs to deal with the problems that come up in the digital afterlife?

III. Conceptual Framework: Digital Identity and Rights After Death

A legal inquiry into the digital afterlife necessitates a comprehensive understanding of the composition of digital assets and the rights associated with them. Digital assets encompass a diverse range of intangible resources, including social media accounts on platforms such as Meta Platforms, electronic mail, cryptocurrency holdings, cloud-stored data, digital photographs, and online subscriptions to various forms of electronically maintained information. It can be hard to put these assets into traditional legal categories of property because they may have economic value, sentimental value, or evidentiary value.

Digital assets are not usually owned in the same way that physical property is. Instead, they live in contracts between the user and the service provider. The terms of service often say that assets can't be transferred, which makes it unclear whether succession law allows them to go to legal heirs. This contractual overlay creates a fragmented legal situation in which the user's ability to control their digital presence during their lifetime does not easily translate into rights that can be passed down.

On a deeper conceptual level, the idea of digital identity has developed as an extension of personal identity and autonomy. A person's digital footprint, which includes their communications, photos, preferences, and recorded interactions, is a virtual version of who they are. In legal terms, this is similar to the doctrine of personality rights, which protects parts

ISSN: 2582-6433

of a person's identity from being taken or used without permission. The digital realm obscures the boundary between property and personhood, as digital assets represent not only economic commodities but also manifestations of individual dignity.[1]

This situation raises the important question of posthumous privacy: does the right to privacy still apply after a person dies? Conventional legal thought has predominantly maintained that privacy, as a personal right, ceases to exist upon death. But in the digital world, this position doesn't seem strong enough. Data lasts for a long time, and using it wrong can hurt not only the reputation and dignity of the dead person, but also the interests of the family members who are still alive. The increasing acknowledgment of informational privacy as a facet of human dignity indicates that specific aspects of privacy may warrant posthumous protection, even in the absence of explicit legislative directives.[2][3]

A major source of tension comes from the conflicting claims that can be made over digital assets. On one side are the interests of heirs and legal representatives, who may want access for reasons like managing the estate, keeping sentimental items safe, or making money. On the other hand, there is the deceased person's right to privacy, which could include a wish, either spoken or unspoken, to keep personal information private or limit access to it. This conflict reveals a fundamental normative quandary: whether digital assets should be regarded as inheritable property regulated by succession law, or as extensions of personal autonomy that warrant respect post-mortem.

Without a clear legal framework, this tension remains unresolved, leading to inconsistent practices and fostering conditions ripe for abuse. A principled legal response must reconcile proprietary interests with personality rights, while also considering the contractual obligations established by digital service providers. This kind of framework would have to find a way to make digital identity fit with established ideas about succession and privacy. This would make it easier to regulate digital rights after death.

[1] Edina Harbinja, *Legal Status of Digital Assets: Is There a Need for a New Category of Property?*, 7 Masaryk U. J.L. & Tech. 211 (2013).
[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) (recognizing the right to privacy as a fundamental right under Article 21 of the Constitution of India).
[3] Natalie M. Banta, *Death and Privacy in the Digital Age*, 94 N.C. L. Rev. 927 (2016).

ISSN: 2582-6433

IV. The Current Legal System In India

India's rules about digital assets are still not very good, especially when it comes to who owns and controls them after death. The current legal framework does not directly address the notion of a digital afterlife, resulting in significant uncertainty regarding the rights, obligations, and liabilities associated with the data of deceased individuals.

The Information Technology Act, 2000 is India's main law that controls cyber activities. It sets the rules for dealing with crimes like unauthorized access, identity theft, and data breaches. But it is very quiet about what happens to digital assets after someone dies. There is no law that says whether a legal heir who wants to get into a deceased person's digital accounts is doing so legally or illegally. Because of this, family members who try to get back or manage this kind of data may, in some cases, be breaking the law and could be held legally responsible. This silence in the law shows that people didn't think about how digital identities last long after the people who made them die.[4]

The Indian Succession Act of 1925, which governs how property is divided after death, is also hard to understand when it comes to digital assets. The Act is based on physical property and well-known types of intangible assets that can be clearly owned and transferred. However, digital assets don't fit into these categories very well. Assets with economic value, like cryptocurrency or monetized accounts, could be considered part of the deceased person's estate. However, personal data, like private messages, photos, and social media interactions, brings up important questions about whether it can be passed down. The lack of clear legal recognition makes it very unclear whether this kind of data goes to heirs or is not part of the succession at all.[5]

The Digital Personal Data Protection Act, 2023, is the most recent example of India's changing data protection laws. They don't say much about posthumous rights. The main goal of the Act is to protect the personal information of living people. It doesn't say anything about protecting the information of dead people. The issue of the persistence of privacy rights post-mortem remains significantly unresolved. While some broad principles, like limiting the use of data and keeping it safe, may affect how posthumous data is handled, there are no official rules for

[4] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[5] Indian Succession Act, 1925, No. 39, Acts of Parliament, 1925 (India).

ISSN: 2582-6433

enforcing posthumous privacy rights or clear ways to do so.[6]

In practice, the rules that govern digital assets are mostly based on the terms of the contracts that service providers make. Companies like Google LLC and Meta Platforms run platforms that have very detailed terms of service that usually include rules about what happens to a user's account when they die, such as account termination, memorialization, or restricted access. These terms of the contract usually don't allow the transfer of account rights, and they may also override claims made by legal heirs under domestic succession law. So, even if heirs have a good reason to want to access digital assets, their rights depend on the rules and choices of private companies. This effectively gives private individuals control over the digital afterlife, which leads to inconsistencies and a clear lack of common legal standards.[7]

Indian legal system has a big gap in its rules and norms for what happens to digital assets after someone dies. There is legal uncertainty and the possibility of injustice because there are no specific laws, existing laws have their own problems, and private contracts take precedence. There is an urgent need for a comprehensive and coherent legal framework that integrates cyber law, succession law, and data protection principles to effectively regulate posthumous digital rights.

V. Cyber Crimes in the Context of the Digital Afterlife

The ongoing existence of digital data after a person's death has led to a unique category of cyber crimes in which the identity and digital information of deceased individuals are misused for illegal purposes. The lack of a clear legal framework for posthumous digital rights increases the risk of misuse of such data in many ways.

One of the most common ways this happens is when someone steals the identity of the dead person. Criminals may steal the digital credentials of a dead person and use them to impersonate that person, doing things like making fake online profiles, sending unauthorized messages, or artificially extending the person's digital presence for dishonest reasons. Financial fraud is very similar. In this case, criminals get into the deceased person's bank accounts, email

[6] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[7] Meta Platforms, Inc., *Memorialization Request*, Facebook Help Center, https://www.facebook.com/help/1506822589577997 (last visited Apr. 14, 2026); Google LLC, *About Inactive Account Manager*, Google Account Help, https://support.google.com/accounts/troubleshooter/6357590 (last visited Apr. 14, 2026).

ISSN: 2582-6433

accounts, or digital wallets to steal money or change financial information. A breach of one digital account can lead to unauthorized access to other connected services because many digital accounts are linked to each other.

Another big worry is that people are pretending to be dead people on social media, especially on sites run by companies like Meta Platforms, where inactive accounts can stay active or be fraudulently reactivated. People can use impersonation to lie, hurt someone's reputation, or emotionally manipulate the deceased's friends and family. The unauthorized use of personal photos and other information, such as digital manipulation, unauthorized publication, or commercial exploitation, is also very worrying for the deceased's dignity and reputation.

Even though these actions are clearly very serious, it is very hard to put them into categories under Indian law. The Information Technology Act of 2000 punishes crimes like stealing someone's identity, cheating by pretending to be someone else, and getting into a computer without permission. These rules, on the other hand, are mostly about harm done to living people. When the victim is dead, it is legally unclear whether the relevant acts fit the legal definitions, especially if the crime assumes that there is a "person" who can be harmed or tricked. This creates problems when it comes to interpreting existing laws to include harms that happen after death, which means that some types of bad behavior are not covered by the law.[8]

Enforcement of these offenses is further impeded by evidentiary challenges. It is harder to show unauthorized access or misuse after the person whose data was stolen has died because you have to prove ownership, consent, and identity. After death, verifying a person's digital identity raises the question of who has the legal right to represent the deceased's interests or give permission for others to access their data. The lack of legal recognition for digital executors or designated representatives for digital assets makes the process of gathering evidence even more difficult. Digital evidence can also be changed, deleted, or encrypted, which can make it less reliable and less likely to be accepted by a court.[9][10]

[8] Information Technology Act §§ 66C, 66D, 2000 (India) (penalizing identity theft and cheating by impersonation using computer resources).
[9] Information Technology Act § 43A, 2000 (India) (providing for compensation for failure to protect sensitive personal data); *see also* Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).
[10] Lilian Edwards & Edina Harbinja, *Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World*, 32 Cardozo Arts & Ent. L.J. 83 (2013).

ISSN: 2582-6433

In essence, cyber offences arising in the context of the digital afterlife reveal significant lacunae in both substantive and procedural law. The existing frameworks' failure to properly categorize these offenses and address evidentiary issues indicates a pressing necessity for reform. A credible legal response must broaden the scope of cybercrime legislation to encompass the posthumous exploitation of data, while also instituting explicit protocols for authentication, authorized access, and legal representation, thereby promoting effective enforcement and safeguarding digital dignity post-mortem.

VI. Different Legal Points of View

A survey of foreign jurisdictions indicates that the legal treatment of digital assets post-mortem is inconsistent, with varying approaches that highlight conflicting priorities among property rights, privacy concerns, and contractual freedom. Some countries have passed laws that deal specifically with digital estate management, while others mostly rely on data protection principles or tools that private platforms have come up with.

The US has taken a more direct approach to the issue of the digital afterlife through legislation. The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) is the most important law that sets up a structured way for fiduciaries, such as executors and trustees, to access and manage the digital assets of people who have died. The law tries to balance the needs of the deceased, their survivors, and service providers by recognizing fiduciary authority, but only with the user's permission and according to the rules that govern the account. RUFADAA is important because it introduces the idea of digital estate planning, which lets people write down how they want their digital assets to be handled after they die. In the United States, however, the law is applied differently in each state, and service providers have a lot of leeway in their contracts, which makes it harder to be consistent.[11]

The European Union, on the other hand, mostly looks at the problem through the lens of data protection. The General Data Protection Regulation (GDPR) establishes a comprehensive framework for safeguarding personal data, grounded in the principles of privacy, informed consent, and informational self- determination. The GDPR only protects living people, though, and its protections don't automatically apply to people who have died. Some Member States

[11] Revised Uniform Fiduciary Access to Digital Assets Act (2015), Unif. Law Comm'n (2015), https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728- 81c6-b39a91ecdf22.

ISSN: 2582-6433

have passed extra laws that recognize limited posthumous data rights, especially when it comes to the deceased person's wishes and the claims of surviving family members. This creates a mixed framework in which privacy concerns still matter after death, but there is no consistent, enforceable right at the supranational level.[12][13]

Digital platforms have also created their own ways to handle accounts after a user dies, in addition to legal documents. Meta Platforms and Google LLC are two companies that have made policies that allow people to memorialize, delete, or limit access to their accounts. For example, social media accounts can be turned into memorialized profiles, which keep the content that is already there but stop people from using them actively. Some platforms let users choose a legacy contact or set up automated account management if they don't use the account for a long time. These mechanisms provide practical solutions; however, they are contractual and discretionary, lacking the authority of statutory entitlements and differing significantly across platforms.

The comparative analysis thus shows that there is a clear lack of coherence at the international level. The United States focuses on fiduciary access and digital estate planning, while the European Union focuses on data protection without fully addressing posthumous rights. Private platforms fill in the gaps in regulation with their own policies. This disjointed and inconsistent global landscape highlights the lack of a universally recognized legal principle governing digital assets post-mortem. It also shows that places like India need to create a balanced and complete legal system that includes parts of succession law, privacy protection, and contract law, while making sure that the law is clear, consistent, and easy to follow.

VII. Important Legal and Moral Questions

The management of digital assets within the framework of the digital afterlife raises complex legal and ethical dilemmas that contest traditional principles of property, privacy, and individual autonomy. These questions are at the intersection of conflicting interests and require a careful, principled answer.

A key point of disagreement is the difference between access and ownership. The legal status

[12] Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[13] GDPR, *supra* note 6, recital 27 (stating that the Regulation does not apply to the personal data of deceased persons, but leaves it to Member States to provide rules for such processing).

ISSN: 2582-6433

of digital data as either a form of property eligible for inheritance or as an extension of personality rights that is inherently non- transferable remains unresolved. Some digital assets, especially those with clear economic value, can be compared to known types of property. A substantial portion of digital data, encompassing private correspondence, personal photographs, and social media interactions, is intrinsically linked to an individual's identity and autonomy, rendering its classification as heritable property highly problematic. This dual nature makes it harder to apply succession law in a straightforward way, since giving heirs full ownership rights may not be in line with the personal aspects of such data. So, it might be better to recognize a limited right of access instead of full ownership.

The issue of consent after death is very similar. A significant issue pertains to whether consent given by an individual during their lifetime should dictate the posthumous administration and utilization of their digital assets. In theory, tools like advance directives or digital wills could be used to express this kind of consent. However, without clear instructions, trying to figure out what the deceased wanted is always a risky business. Even if consent has been recorded, there may still be questions about its scope, enforceability, and whether it meets the platform's contractual requirements. This makes prior consent an inadequate tool for fully controlling the use of digital data after death.

Another important issue is that digital platforms have too much power over who can access and manage digital assets. Companies like Meta Platforms and Google LLC have a lot of power because of the terms of service they set. These terms often decide what happens to user accounts after they die and can even override the rights of legal heirs under domestic law. This privatization of regulation raises significant concerns about accountability, transparency, and the power imbalance between users and service providers.

From an ethical perspective, the dignity of the deceased is a paramount consideration. Unauthorized use or disclosure of a deceased individual's data can damage their reputation, alter their memory, and breach their personal integrity. The law has historically focused on the rights of living individuals; however, the digital context necessitates a reevaluation of whether the notion of dignity should transcend death, especially in cases where damage to legacy and reputation is apparent.

Finally, we can't ignore how the death affected the family members who are still alive. Access

ISSN: 2582-6433

to a deceased individual's digital assets may hold significant sentimental value for relatives, allowing them to preserve memories or attain a sense of closure. At the same time, unrestricted access could reveal very private information that the deceased may not have wanted to share. This creates an ethical conflict between respecting privacy and meeting the emotional needs of the bereaved.

The legal and ethical aspects of the digital afterlife exemplify a significant evolution in the concepts of identity, property, and privacy in the digital era. To meet these challenges, we need to carefully balance private interests, personal freedom, corporate responsibility, and human dignity. This needs to be done within a clear and forward-looking legal framework.

VIII. The Need for Legal Recognition of Digital Inheritance

The rapid growth of digital technology has fundamentally changed the nature of personal property, forcing legal systems to rethink how to handle digital data after its owner dies. Because there isn't a clear set of laws about how to inherit and manage digital assets, there is a lot of confusion. This shows how important it is to have formal legal recognition of the idea of digital inheritance.

There are strong reasons to consider some types of digital assets as property that can be passed down. Digital assets like cryptocurrency portfolios, monetized social media accounts, digital intellectual property, and online bank accounts all have real-world economic value. From the perspective of succession law, these assets closely resemble traditional types of intangible property and should, in theory, be included in the deceased's estate. Recognizing digital assets as inheritable would enable legal heirs and executors to manage these assets in accordance with the established principles of the Indian Succession Act, 1925. This would also bring predictability and prevent situations where valuable digital resources become inaccessible or are lost due to technical barriers or restrictive platform policies.[14]

However, recognizing digital inheritance is not without its challenges. Concerns about privacy and confidentiality are the main reason for the objection. Digital accounts often hold very private information, like private messages, personal photos, and other data, that the deceased may not have wanted to share with anyone, even close family members. If you treat all of this

[14] Indian Succession Act §§ 211–227, 1925 (India) (governing the duties, powers, and liabilities of executors and administrators in the administration of the estates of deceased persons).

ISSN: 2582-6433

information as inheritable property, it could hurt the deceased's freedom and dignity. Also, digital platforms often have strict confidentiality rules in their contracts that make it hard to share or move account content. These issues show that traditional ideas about property don't always work for digital assets that have both economic value and very personal information.

Because of these conflicting factors, a balanced legal approach is needed. A hybrid model that takes into account both proprietary and personality interests in digital assets is one possible solution. With this plan, assets that have clear economic value could be passed down to legal heirs according to succession law. On the other hand, data that mostly shows personal identity, like private messages and social media interactions, could be protected by privacy and personality rights, which would put real limits on unrestricted access.

This kind of mixed approach would let the law balance the economic reality of digital assets with the moral obligation to respect people's freedom. It would also set up a way for people to control their digital legacy while they are still alive, such as by making digital wills or naming digital executors. In the end, a balanced legal framework that formally recognizes digital inheritance would make the law more certain, protect the dignity of the deceased, and make sure that digital assets are taken care of responsibly as society continues to move into the digital age.

IX. Problems and Gaps in Policy

Even though digital assets are becoming more and more important in everyday life, India's rules about the digital afterlife are full of big policy gaps and practical problems. These flaws make it harder for the law to be enforced and make people, legal heirs, and institutions that have to deal with digital data after death less sure of what to do.

A primary issue is the lack of statutory clarity. Current laws, like the Information Technology Act of 2000 and the Indian Succession Act of 1925, do not clearly say what happens to digital assets after someone dies, who owns them, or how they can be transferred. This gap in the law leads to different interpretations, which makes it hard for courts and parties to know what to do. As a result, problems with access, control, and liability are solved on an ad hoc basis, which goes against the predictability and legal certainty that a mature legal system needs.

Another problem is that most users don't know about it. Most people don't do any kind of

ISSN: 2582-6433

digital estate planning, and they also don't know enough about what happens to their digital assets when they die. The lack of widely used tools like digital wills, legacy contacts, or account management directives makes things hard for family members who are still alive. This lack of information makes the legal situation even more unclear, since the preferences and wishes of the deceased are rarely written down in a way that is easy to find or enforce.

Cross-border jurisdictional issues make the situation even more complicated. Digital assets are often stored on servers located outside of India and are subject to foreign laws as well as the contractual terms of multinational corporations like Google LLC and Meta Platforms. This causes conflicts of law, especially when Indian privacy and succession laws are different from those of the foreign jurisdiction that applies. Enforcing rights across borders becomes a difficult task because it involves complicated issues of applicable law, jurisdictional authority, and the availability of international cooperation mechanisms.

Lastly, technological barriers to access and recovery are a real problem that can make it hard for even legally entitled heirs to get what they are owed. Encryption, multi-factor authentication, and other strict security measures are usually used to protect access to digital accounts. If heirs don't have the right account information or an authorized way to access it, they may not be able to get or manage digital assets even though they have the legal right to do so. Additionally, service providers may refuse to grant access in accordance with their own privacy policies, which makes recovery efforts even harder.

When you look at all of these policy gaps and real-world problems together, they show that the system isn't doing a good job of dealing with the realities of the digital afterlife. The combination of legal uncertainty, a lack of public knowledge, complicated jurisdictional issues, and technological limitations makes a strong case for a comprehensive and harmonized framework. This framework should provide legal clarity, raise user awareness, make cross-border cooperation easier, and include practical technological solutions for the fair management of digital assets after death.

X. Suggestions and Ideas for Change

The analysis in the previous sections shows that India's laws about the digital afterlife are not only not enough, but also not connected. To deal with the growing problems that come with digital assets and managing data after death, we need a complete, forward-looking plan for

ISSN: 2582-6433

reform. The following suggestions are made to make sure that this quickly changing area is clear, accountable, and well-protected of rights.

First and foremost, there is an urgent need for specific laws on digital inheritance. A specific set of laws should spell out what digital assets are, how they are classified, and how they can be passed on after death. Such legislation should align the tenets of succession law, privacy, and cyber law, resolving current ambiguities and creating a uniform standard for courts, individuals, and service providers.

This is closely related to the need to formally recognize posthumous data rights. The law should clearly say that some aspects of privacy and personal dignity do not go away when someone dies. Such recognition would give the law a reason to protect against unauthorized access, misuse, or exploitation of a dead person's data, as well as protect the reputational interests and concerns of surviving family members.

Also, there should be mandatory ways to nominate people for digital accounts. Digital platforms should be required to let users choose a nominee or legacy contact who can access or manage their accounts after they die, just like banks and other financial institutions are required to do. This kind of system would make things less uncertain, make it easier to move digital assets, and make sure that the user's wishes are followed.

Another important change is to make sure that platform policies follow national law. At the moment, companies like Google LLC and Meta Platforms have too much power because their terms of service often override people's legal rights in their own countries. Legislative intervention is necessary to guarantee that these policies align with statutory rights, especially regarding access for legal heirs and the safeguarding of posthumous privacy.

It is also important to officially recognize the Digital Executor's role. This would mean creating a legal group of people who are allowed to manage and control the digital assets of a dead person, similar to how executors work under traditional succession law. Such acknowledgment would enable lawful access, mitigate evidentiary challenges, and guarantee the systematic management of digital estates.

From a criminal law point of view, the Information Technology Act, 2000's cyber crime

ISSN: 2582-6433

provisions need to be made stronger so that they clearly cover crimes that involve misusing data from dead people. This would mean changing the definitions of identity theft, unauthorized access, and data misuse to include cases that happen after death. This would close existing gaps and make enforcement more effective.

Lastly, we need to actively encourage people to make digital wills and learn about digital estate planning. People should be urged to write down their wishes about how their digital assets should be managed, moved, or deleted. Public awareness campaigns, legal literacy programs, and the integration of digital wills into estate planning practices would significantly contribute to facilitating informed decision-making prior to the point at which such choices become unfeasible.[15]

The regulation of digital inheritance necessitates a balanced, multifaceted strategy that harmonizes property interests with personal rights, while simultaneously tackling the technological and jurisdictional challenges inherent to the digital realm. If these suggested changes are put into action correctly, they would not only fill in the gaps in the law that already exist, but they would also create a strong framework that can protect digital dignity and make sure that everyone has a fair chance to inherit in the digital age.

XI. Conclusion

The digital age has made it possible for people to live on in a lasting virtual world, which has made the digital afterlife a real and growing issue. As people leave behind huge amounts of digital information over the course of their lives, the need to control that information after they die has become more and more important. But there is still a big hole in the law. The Information Technology Act of 2000 and the Indian Succession Act of 1925 are two examples of laws that don't do a good job of protecting digital data after death. This leaves that data open to more cyber threats, like identity theft and other forms of misuse.

To deal with these problems and make sure that a person's digital dignity is protected after death, there is an urgent and strong need for proactive, coherent legal reform.

[15] Shyamkrishna Balganesh, *The Obligatory Structure of Copyright Law: Unbundling the Wrong of Copying*, 125 Harv. L. Rev. 1664 (2012); *see also* Pranesh Prakash, *Digital Estate Planning in India: An Emerging Imperative*, 5 Indian J. L. & Tech. 45 (2022).

ISSN: 2582-6433

"The law must keep up with technology so that death doesn't take away a person's dignity in the digital world."