JUSTISI

Vol. 12, Issue. 3, September 2026
e-ISSN: 2686-0821, p-ISSN: 1979-7532
https://doi.org/10.33506/js.v12i3.5733
https://ejournal.um-sorong.ac.id/index.php/js/article/view/5733

Article History
Received: 04 June 2026
Reviewed: 22 Aug 2026
Accepted: 16 Sep 2026
Published: 21 Sep 2026

Post-Mortem Digital Identity Abuse in Notarial Systems: Legal Gaps and Cyber Governance Reform

Nafiza Fauziah[1*], Ghaitza Zahira Sofa[2], Pithasari[3], Rifki Agil Ruslan[4]
[1,2,3,4] Faculty of Law, Universitas Airlangga, Indonesia
*correspondence email : nafizafauziah153@gmail.com

Abstract

This study aims to analyze the legal vacuum surrounding post-mortem misuse of notarial digital identities, assess the validity of deeds generated through unauthorized access to deceased notaries' credentials, and formulate a cyber governance framework.

This study employs normative legal research using statutory and conceptual approaches, focusing on notarial authority, authentic deeds, electronic authentication, data protection, cybersecurity, and notarial protocols following a notary's death.

The novelty of this research lies in conceptualizing ghost deeds as a form of post-mortem digital identity abuse arising from the disconnection between the legal termination of notarial authority and the technical operability of digital credentials.

The results of the research indicate that Indonesian law remains focused on the physical transfer of notarial protocols and does not adequately regulate the deactivation, supervision, and audit of deceased notaries' digital credentials. Consequently, electronic systems may create an appearance of authenticity despite the absence of valid legal authority. Ghost deeds should therefore be classified as null and void due to a fundamental defect of authority.

The conclusion of this study is that Indonesia requires a cyber governance framework incorporating automatic credential deactivation, strengthened digital identity certification, interoperable databases, cybersecurity audits, traceable authentication records, and clear civil, administrative, and criminal liability.

Keywords: Notary Digital Identity; Ghost Deed; Electronic Authentication; Post-Mortem Digital Credentials; Cyber Governance

Abstrak

Penelitian ini bertujuan *untuk menganalisis kekosongan hukum terkait penyalahgunaan identitas digital notaris setelah kematian, menilai keabsahan akta yang dibuat melalui akses tanpa kewenangan terhadap kredensial notaris yang telah meninggal, serta merumuskan kerangka tata kelola siber.*

Penelitian ini menggunakan *metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual, yang berfokus pada kewenangan notaris, akta autentik, autentikasi elektronik, pelindungan data, keamanan siber, dan protokol notaris setelah notaris meninggal dunia.*

Kebaruan *penelitian ini terletak pada konseptualisasi akta semu pascakematian sebagai bentuk penyalahgunaan identitas digital pascakematian yang timbul akibat terputusnya hubungan antara berakhirnya kewenangan hukum notaris dan masih berfungsinya kredensial digital secara teknis.*

Hasil penelitian *menunjukkan bahwa hukum Indonesia masih berfokus pada penyerahan fisik protokol notaris dan belum mengatur secara memadai penonaktifan, pengawasan, serta audit terhadap kredensial digital notaris yang telah meninggal. Akibatnya, sistem elektronik dapat menciptakan kesan autentik meskipun tidak terdapat kewenangan hukum yang sah. Oleh karena itu, ghost deeds harus dinyatakan batal demi hukum karena mengandung cacat mendasar dalam kewenangan.*
Kesimpulan penelitian *ini adalah bahwa Indonesia memerlukan kerangka tata kelola siber yang mencakup penonaktifan kredensial otomatis**,** penguatan sertifikasi identitas digital, basis data antarlembaga nasional yang terintegrasi, audit keamanan siber, rekam autentikasi yang dapat ditelusuri, serta pertanggungjawaban perdata, administratif, dan pidana yang jelas.*
Kata Kunci: *Identitas Digital Notaris; Akta Fiktif; Otentikasi Elektronik; Kredensial Digital Pasca-Kematian; Tata Kelola Siber*

1. INTRODUCTION

The rapid digital transformation of legal and administrative systems has fundamentally reshaped the practice of notarial services across civil law jurisdictions. In Indonesia, the adoption of electronic licensing, digital signatures, and centralized databases has altered the traditional foundations of legal authentication. What was once grounded in physical presence, handwritten signatures, and documentary formalism is increasingly mediated by digital infrastructures. These developments undoubtedly enhance efficiency and accessibility, yet they simultaneously introduce new layers of risk that were largely absent in conventional notarial environments. As technology expands the reach of legal services, it also tests the resilience of institutions responsible for ensuring authenticity and public trust.[1]

Within the civil law tradition, notaries have long functioned as gatekeepers of legal certainty. Their authority rests on strict procedural safeguards, particularly identity verification, the personal appearance of parties, and adherence to formal requirements that distinguish authentic deeds from ordinary documents. This institutional role has historically provided stability in private transactions and has reinforced confidence in contractual relations. However, the increasing reliance on digital identity and electronic verification mechanisms challenges the conventional assumptions underlying the authenticity of notarial deeds.[2] The shift from physical to digital authentication requires a re-evaluation of how trust is constructed in modern legal systems.

In recent years, an emerging and deeply concerning phenomenon has attracted attention among practitioners and regulators, namely the misuse of digital identities belonging to deceased notaries. In practice, electronic accounts, digital certificates, and authentication tools may remain active even after the death of a notary, enabling unauthorized individuals to generate documents under the appearance of formal legality. Such documents, often referred to as "ghost deeds," may not immediately raise suspicion, as they carry the outward features of authenticity. This phenomenon is not merely hypothetical; anecdotal

[1] Roger Brownsword, Law, Technology and Society (Abingdon: Routledge, 2019), 23–25.
[2] John Henry Merryman and Rogelio Pérez-Perdomo, The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America, 3rd ed. (Stanford, CA: Stanford University Press, 2007), 112–14.

evidence from legal practice indicates that unauthorized access credentials, retained tokens, and weak supervisory controls create opportunities for systematic abuse.[3]

The implications of this misuse extend far beyond individual disputes. Digital systems, unlike traditional document-based protocols, allow fraudulent transactions to occur on a larger scale and within shorter periods of time. Unauthorized use of notarial identity may facilitate credit fraud, unlawful land transfers, and corporate manipulation. These risks directly threaten financial stability and property rights, particularly in jurisdictions where authentic deeds play a central evidentiary role. As modern transactions increasingly rely on digital infrastructures, the potential harm resulting from identity misuse becomes more severe and difficult to detect.[4]

The urgency of addressing this issue is further amplified by the global emphasis on the role of legal professionals in preventing money laundering and illicit financial flows. International regulatory frameworks, including those promoted by the Financial Action Task Force, emphasize that notaries are key actors in safeguarding the integrity of financial systems. Weak identity governance, especially in post-mortem situations, creates blind spots that may be exploited by organized crime. This demonstrates that the problem of ghost deeds should not be viewed solely as a professional or administrative matter but as part of a broader challenge in digital governance and regulatory compliance.[5]

Despite the magnitude of these risks, the Indonesian legal framework remains largely silent on the management of digital identity following the death of a notary. The Law on Notarial Office primarily regulates the physical transfer of protocols and administrative responsibilities but does not address cybersecurity, digital authentication, or access control. Similarly, existing electronic signature regulations focus on certification and validity without providing automatic revocation mechanisms. This normative gap raises fundamental questions regarding legal certainty, especially in cases where unauthorized documents have already entered circulation.[6]

This legal vacuum also complicates the resolution of disputes involving ghost deeds. Courts may face difficulties in determining whether such documents should be considered null and void, voidable, or merely evidentiary defects. The absence of clear doctrinal guidance creates inconsistent judicial outcomes and increases litigation risks. Moreover, the allocation of responsibility remains unclear. Questions arise regarding the liability of unauthorized users, supervisory authorities, custodians of notarial protocols, and even digital certification providers. The uncertainty not only weakens legal protection but also exposes innocent third parties to significant harm.

---

[3] Daniel J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008), 98–100.

[4] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Cheltenham: Edward Elgar Publishing, 2015), 76–79.

[5] Financial Action Task Force, *Guidance for a Risk-Based Approach for Legal Professionals* (Paris: FATF, 2019), 37–41.

[6] See Republic of Indonesia, Law No. 30 of 2004 concerning the Office of Notary, as amended by Law No. 2 of 2014, arts. 62–65.

Beyond doctrinal ambiguity, the issue reflects a deeper transformation in professional accountability in the digital age. Traditional legal frameworks assume that authority is inseparable from the physical presence and personal responsibility of professionals. However, digital technologies enable identity to persist beyond the individual, creating what scholars describe as post-mortem identity risk.[7] This phenomenon challenges established notions of authenticity and calls for a reconceptualization of responsibility within technologically mediated systems. It also raises ethical and institutional concerns about the limits of professional authority in digital environments.

From a broader socio-legal perspective, the phenomenon of ghost deeds illustrates the emergence of new risks in modern society. As Ulrich Beck suggests, technological progress inevitably generates systemic risks that transcend individual actors and require collective governance.[8] In this context, the misuse of digital notarial identity is not merely a technical problem but a structural challenge that affects institutional trust and regulatory legitimacy. Without effective safeguards, the digital transformation of legal professions may paradoxically weaken the very certainty it seeks to strengthen.

Existing scholarship on the digital transformation of notarial practice can be divided into several principal strands. The first strand focuses on cyber notary systems, electronic deeds, and the modernization of notarial services. These studies primarily examine whether electronic notarization is compatible with the formal requirements of authentic deeds, including the physical appearance of the parties, the reading and signing of deeds before a notary, identity verification, and the evidentiary status of electronic documents. Alkatiri, Putra, and Ongko, for example, emphasize the need for a specific regulatory framework for electronic notarization in Indonesia by comparing its development with systems adopted in other jurisdictions.[9] Similarly, Toruan examines the use of electronic deeds as a means of improving notarial services and preserving notarial archives.[10] Although these studies demonstrate the growing need to modernize Indonesian notarial law, they remain predominantly concerned with the exercise of authority by living notaries and with the validity of deeds created during an active term of office.

A second strand of scholarship addresses the broader legal nature and governance of digital identity. Robles-Carrillo conceptualizes digital identity as a complex legal category that performs the functions of identification, authentication, and authorization, while also emphasizing that digital identity cannot simply be treated as an electronic reproduction of

[7] Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford: Oxford University Press, 2019), 134–36.

[8] Beck, U. (2009). World Risk Society. In J. K. B. Olsen, S. A. Pedersen, & V. F. Hendricks (Eds.), A Companion to the Philosophy of Technology. Wiley-Blackwell. https://doi.org/10.1002/9781444310795.ch88

[9] Naurah Humam Alkatiri, Mohamad Fajri Mekka Putra, and Kyle Ongko, "A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era," *Jambura Law Review* 5, no. 2 (2023): 332–355, https://doi.org/10.33756/jlr.v5i2.19221

[10] Henry Donald Lbn Toruan, "The Importance of Using Electronic Deeds to Facilitate the Service and Storage of Notary Archives," *Jurnal Penelitian Hukum De Jure* 22, no. 4 (2022): 483–498, https://doi.org/10.30641/dejure.2022.V22.483-498

physical identity.[11] This literature is highly relevant because it demonstrates that digital credentials may continue to operate independently from the physical person to whom legal authority was originally attached. Nevertheless, general studies of digital identity do not specifically examine professional identities belonging to public officials whose electronic credentials can be used to produce legally consequential documents after their authority has ended.

A third strand examines digital remains, post-mortem privacy, digital afterlife technologies, and the persistence of personal data following death. Hollanek and Nowaczyk-Basińska demonstrate that data belonging to deceased persons may be collected and reused to create post-mortem digital representations, thereby generating ethical risks for the deceased, data holders, and third-party users.[12] More recently, Cunneen and colleagues conceptualize human digital remains as including online profiles, biometric data, behavioural traces, and other digital representations that continue to exist after biological death. They argue that the persistence and potential commodification of such data require anticipatory governance because existing legal frameworks do not adequately address their posthumous use.[13] These contributions establish that death does not automatically terminate the technical existence or accessibility of digital identity. However, their analysis is primarily directed toward privacy, dignity, digital replicas, artificial intelligence, and personal data rather than the continued use of professional credentials to exercise public authority.

Accordingly, a significant research gap exists at the intersection of notarial authority, post-mortem digital identity, and cybersecurity governance. Previous studies on cyber notaries have concentrated on electronic deeds, remote appearance, electronic signatures, and the compatibility of digital procedures with conventional formalities. Studies on digital identity have examined its conceptual and regulatory dimensions, while post-mortem digital scholarship has predominantly addressed privacy, digital legacy, and artificial representations of deceased persons. These bodies of literature have not adequately explained how the legal termination of a notary's authority should be synchronized with the technical revocation of electronic certificates, authentication tokens, passwords, and institutional access credentials.

Furthermore, previous research has not systematically addressed the legal status of deeds generated after the death of a notary through the unauthorized use of still-active credentials. It has also not clearly allocated responsibility among unauthorized users, custodians of notarial protocols, supervisory authorities, electronic certification providers, and administrators of governmental digital platforms. The unresolved issue is therefore not merely whether electronic notarization should be recognized, but how the legal system should

[11] Margarita Robles-Carrillo, "Digital Identity: An Approach to Its Nature, Concept, and Functionalities," *International Journal of Law and Information Technology* 32 (2024): eaae019, https://doi.org/10.1093/ijlit/eaae019

[12] Tomasz Hollanek and Katarzyna Nowaczyk-Basińska, "Griefbots, Deadbots, Postmortem Avatars: On Responsible Applications of Generative AI in the Digital Afterlife Industry," *Philosophy & Technology* 37 (2024): 63, https://doi.org/10.1007/s13347-024-00744-w

[13] Máirtín Cunneen, Ruhi AnandFinn, Raymond Friel, Paul Tennent, and Sami Brandt, "From Bones to Bytes: Anticipating and Addressing the Governance Challenges of Human Digital Remains and Posthumous Digital Human Twins," *AI & Society* 41 (2026): 2021–2040, https://doi.org/10.1007/s00146-025-02514-4

respond when an apparently valid digital authentication is produced by an identity whose underlying public authority has already ceased.

This research fills that gap by conceptualizing ghost deeds as a distinct form of post-mortem professional identity abuse. Unlike ordinary identity theft, the misuse of a deceased notary's digital identity may create documents carrying the appearance and evidentiary consequences of public authority. The novelty of this study therefore lies in connecting the termination of notarial authority with the lifecycle governance of digital credentials and in proposing an integrated cyber governance framework consisting of automatic credential deactivation, institutional database interoperability, strengthened identity certification, mandatory cybersecurity audits, traceable authentication records, and a clearer allocation of civil, administrative, and criminal liability.

Against this background, this article argues that ghost deeds reflect a structural failure to synchronize the legal termination of professional authority with the technical lifecycle of digital identity. Addressing this problem requires an integrated framework combining notarial law, cybersecurity, digital identity governance, and institutional oversight. Digital credential management must therefore be treated as an essential component of professional accountability rather than merely as a technical or administrative concern.

Accordingly, this study examines three central issues. First, it analyzes the legal vacuum in regulating post-mortem digital identity and access control within the Indonesian notarial system. Second, it evaluates the legal validity and liability implications arising from the misuse of deceased notaries' identities. Third, it proposes a forward-looking model of cyber governance aimed at strengthening institutional resilience and protecting public trust.

The proposed framework emphasizes preventive and systemic solutions, including automatic digital deactivation, strengthened certification mechanisms, cybersecurity audits, and clearer allocation of liability. By integrating legal and technological strategies, the model seeks to reinforce trust in authentic deeds while ensuring adaptability in a rapidly evolving digital environment. Ultimately, this research contributes to the modernization of notarial law by addressing an overlooked but increasingly urgent issue in contemporary legal practice.

2. METHOD

This study employs a normative legal research method, understood as doctrinal inquiry directed at identifying, interpreting, systematizing, and evaluating legal norms applicable to the misuse of deceased notaries' digital identities.[1] The research does not seek to measure the empirical frequency of such misuse, but rather to determine its legal implications and to identify gaps between the legal termination of notarial authority and the technical lifecycle of digital credentials. Two principal approaches are employed: a statutory approach and a conceptual approach. The statutory approach examines the Indonesian Civil Code, Law Number 30 of 2004 concerning the Office of Notary as amended by Law Number 2 of 2014, Law Number 11 of 2008 concerning Electronic Information and Transactions as most recently amended by Law Number 1 of 2024, Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions, Minister of Communication and

Informatics Regulation Number 11 of 2022 concerning Governance of Electronic Certification, and Law Number 27 of 2022 concerning Personal Data Protection. The conceptual approach is used to examine the principles of legal certainty, public authority, authenticity of legal instruments, professional responsibility, digital identity, and cyber governance.

The analysis is structured through three interrelated normative tests. First, legal validity is assessed by examining whether a purported notarial act satisfies the requirements relating to the competent public official, the prescribed form and procedure of an authentic deed, and the legal status of the notary at the time the act is attributed to that notary. Particular attention is given to Article 1868 of the Indonesian Civil Code and the provisions of the Notarial Office Law governing notarial authority and the formal requirements of notarial deeds. Second, defects of authority are examined by comparing the legal duration of notarial authority with the temporal use of the relevant digital identity. Article 8 paragraph (1) letter a of Law Number 30 of 2004 provides that a notary ceases to hold office upon death, while Articles 62 and 63 regulate the subsequent transfer of the notarial protocol. These provisions are used to determine whether the continued technical availability or use of a digital credential can have any legal effect once the personal authority attached to the office has ceased. Third, cyber governance is evaluated by examining the regulatory controls applicable to electronic identity and authentication, including the linkage between an electronic signature and its signatory, control over signature-creation data, validity and revocation of electronic certificates, prevention of unauthorized access, and institutional responsibility for credential management. For this purpose, the study particularly examines Articles 59–62 of Government Regulation Number 71 of 2019 and the electronic certification governance framework under Minister of Communication and Informatics Regulation Number 11 of 2022. The term "ghost deeds" is employed in this study as an analytical construct rather than a statutory legal category, referring to purported notarial instruments generated or authenticated through the digital identity of a notary after the notary's legal authority has terminated.

The legal materials were selected purposively according to four criteria: normative authority, direct relevance to the research problem, regulatory status, and functional connection to the lifecycle of notarial and digital authority. Primary legal materials consist of legislation governing the creation and evidentiary status of authentic deeds, the commencement and termination of notarial authority, custody of notarial protocols, electronic signatures and certificates, electronic-system security, unauthorized electronic access, and the protection or misuse of identity-related data. Secondary legal materials consist of authoritative legal monographs, peer-reviewed journal articles, and doctrinal scholarship concerning notarial law, legal certainty, electronic authentication, digital identity, cybersecurity, and technology governance. Priority is given to sources that directly explain or critically evaluate the legal relationship between authority, authentication, and digital credentials. The materials are analyzed qualitatively through grammatical, systematic, and conceptual interpretation. The analysis proceeds by identifying and classifying the relevant norms, examining their interrelationship across the notarial and electronic-governance regimes, testing their

application to post-mortem credential use, identifying normative inconsistencies or regulatory lacunae, and subsequently constructing prescriptive recommendations. This analytical sequence enables the study to distinguish between legal authority, which terminates according to law, and technical access, which may remain operational unless the relevant digital credential is revoked or disabled, thereby providing the basis for evaluating whether the existing regulatory framework adequately addresses post-mortem misuse of notarial digital identity.

3. DISCUSSION

3.1. Digital Transformation and Cyber Risks in Notarial Practices

The transformation of digital technology has significantly reshaped the institutional landscape of legal services, including the practice of notaries in civil law jurisdictions. Traditionally, the authority of notaries has been closely associated with the formal requirements of authenticity, particularly the personal appearance of parties, the verification of identity through physical documents, and the procedural recording of legal acts. These safeguards were designed to ensure that authentic deeds possess the highest evidentiary value in legal proceedings[14]. However, the rapid expansion of digital infrastructures has gradually altered these traditional mechanisms by introducing electronic systems that mediate identity verification, document authentication, and legal recordkeeping.

In Indonesia, the digitalization of administrative governance has accelerated through the development of electronic platforms and centralized databases administered by state institutions. Notarial activities increasingly intersect with digital systems that facilitate corporate registration, electronic licensing, and other administrative procedures. While such developments promote efficiency and transparency, they also transform the normative framework within which authenticity is constructed. The reliance on digital infrastructures inevitably introduces new layers of technological dependency that were previously absent in conventional paper-based systems[15].

From a normative perspective, the authenticity of notarial deeds is inseparable from the principle of legal certainty.[16] The doctrine of authentic deeds within civil law systems rests upon the presumption that documents produced by authorized officials accurately reflect the legal acts of the parties involved.[17] This presumption is sustained through procedural safeguards that ensure the reliability of identity verification and the integrity of documentation. When authentication mechanisms shift from physical verification to digital credentials, the normative foundations of this presumption must be reconsidered.

One of the most significant developments in this transformation is the emergence of

[14] J.H. Merryman and Rogelio Pérez-Perdomo, The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America, 3rd ed. (Stanford: Stanford University Press, 2007), 112–114.
[15] Roger Brownsword, Law, Technology and Society (Abingdon: Routledge, 2019), 23–25.
[16] Article 1868 and Article 1870 of the Indonesian Civil Code; Law Number 30 of 2004 concerning the Office of Notary, as amended by Law Number 2 of 2014 concerning Amendment to Law Number 30 of 2004 concerning the Office of Notary, particularly Article 1 point 7, Article 15 paragraph (1), Article 39, and Article 44.
[17] Peter Mahmud Marzuki, Penelitian Hukum, rev. ed. (Jakarta: Kencana, 2017), 92–93.

digital identity as a central element in electronic governance. Digital identity refers to the collection of electronic credentials used to verify an individual's legal authority within digital systems. In the context of notarial practice, such credentials may include electronic certificates, login authentication, cryptographic keys, and biometric verification tools.[18] These technologies are intended to replicate the assurance traditionally provided by physical identification processes. However, their effectiveness depends heavily on the integrity of identity management systems.

The integration of electronic authentication systems further reinforces the digital transformation of legal procedures. Electronic signatures and digital certificates are widely recognized as legally valid mechanisms for authenticating documents and verifying the identity of signatories. Through public key infrastructure (PKI), electronic documents can be securely linked to specific individuals and verified through cryptographic processes.[19] This technological framework is designed to ensure that digital documents maintain evidentiary reliability comparable to conventional written instruments.

Despite these advantages, the reliance on electronic authentication systems also introduces significant risks related to identity management. Digital credentials, unlike physical identity verification, can potentially be accessed or manipulated by unauthorized actors if security mechanisms fail. Such vulnerabilities may arise from weak password protocols, compromised authentication tokens, or inadequate oversight of digital certification systems. When these risks intersect with legal authority, particularly the authority of notaries to produce authentic deeds, the consequences may extend beyond technical failures and directly affect legal certainty.

The problem becomes particularly pronounced when digital credentials remain active after the death of a notary. In conventional notarial practice, the death of a notary automatically terminates the authority to produce authentic deeds, and administrative procedures ensure the transfer of protocols to designated custodians. However, digital systems do not necessarily reflect this institutional transition automatically. Without explicit mechanisms for deactivating electronic credentials, digital identities may continue to exist within administrative platforms despite the termination of professional authority.

This situation creates opportunities for the misuse of digital identities belonging to deceased notaries. Unauthorized individuals who gain access to digital credentials may generate documents that appear to satisfy formal authentication requirements. These documents may circulate within legal and administrative systems without immediately revealing their irregular origins. In such circumstances, the outward appearance of authenticity may conceal fundamental defects in authority.

The phenomenon commonly referred to as "ghost deeds" illustrates how technological vulnerabilities intersect with legal authority. Documents produced through unauthorized

[18] Daniel J. Solove, Understanding Privacy (Cambridge, MA: Harvard University Press, 2008), 98–100.
[19] Bart van Looy et al., "Digital Identity and Legal Authentication," *Computer Law & Security Review* 37 (2020): 5–7, https://doi.org/10.1016/j.clsr.2020.105430.

access to a deceased notary's digital identity may resemble legitimate authentic deeds in form and structure. Yet the absence of a valid authority behind such documents raises serious questions regarding their legal validity. From a doctrinal perspective, this situation challenges the traditional assumption that the authenticity of a deed guarantees the legitimacy of the legal act it records.

Technological developments such as artificial intelligence further complicate the risks associated with post-mortem misuse of notarial digital identity. Emerging technologies, including deepfake systems capable of replicating facial expressions, voice patterns, and other biometric characteristics, demonstrate how digital environments can increasingly simulate human presence[20]. This development is particularly relevant to notarial law because the authenticity of a notarial act depends not only on the existence of a document, but also on the lawful exercise of authority by the notary and the reliable identification and participation of the persons appearing before the notary. Where digital notarial processes incorporate video identification, biometric verification, electronic signatures, or other remote authentication mechanisms, synthetic media may undermine those safeguards by creating the appearance that a deceased or otherwise unauthorized individual is still participating in the authentication process. In the specific context of post-mortem misuse, deepfake technology could therefore operate in combination with active digital credentials to reinforce the false appearance that a deceased notary remains personally involved in the creation or authentication of a legal instrument. The relevance of artificial intelligence to this study consequently lies not in the technology itself, but in its capacity to weaken the evidentiary reliability of digital identity verification and to amplify the regulatory gap between the legal termination of notarial authority and the continued technical usability of digital authentication mechanisms.

The growing sophistication of cyber fraud also contributes to the risks surrounding digital identity misuse. Cybercriminals frequently target professional accounts that provide privileged access to legal and financial systems. In Indonesia, such conduct falls within the regulatory framework of Law Number 11 of 2008 concerning Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024, particularly Article 30 concerning unauthorized access to computers and electronic systems, Article 32 concerning unlawful alteration, transfer, or interference with electronic information and documents, and Article 35 concerning the manipulation or creation of electronic information or documents so that they appear to constitute authentic data. The misuse of personal identity data is further regulated under Articles 65 and 66 of Law Number 27 of 2022 concerning Personal Data Protection, with criminal sanctions stipulated in Articles 67 and 68. Because notaries operate at critical points of legal authentication, especially in property transactions, corporate documentation, and financial agreements, their digital credentials represent highly valuable targets for unauthorized exploitation. Compromised credentials may facilitate fraudulent asset transfers, manipulation of corporate records, or the creation of fictitious legal transactions.

These risks reveal a broader structural challenge associated with digital modernization.

[20] Mireille Hildebrandt, Smart Technologies and the End(s) of Law (Cheltenham: Edward Elgar, 2015), 76–79.

As legal institutions adopt technological systems designed to improve efficiency, they must also confront the unintended consequences of technological dependency. Scholars of risk governance have long emphasized that technological innovation often generates new forms of systemic risk that cannot be addressed solely through traditional regulatory frameworks.[21] The emergence of cyber vulnerabilities within notarial systems reflects this broader dynamic.

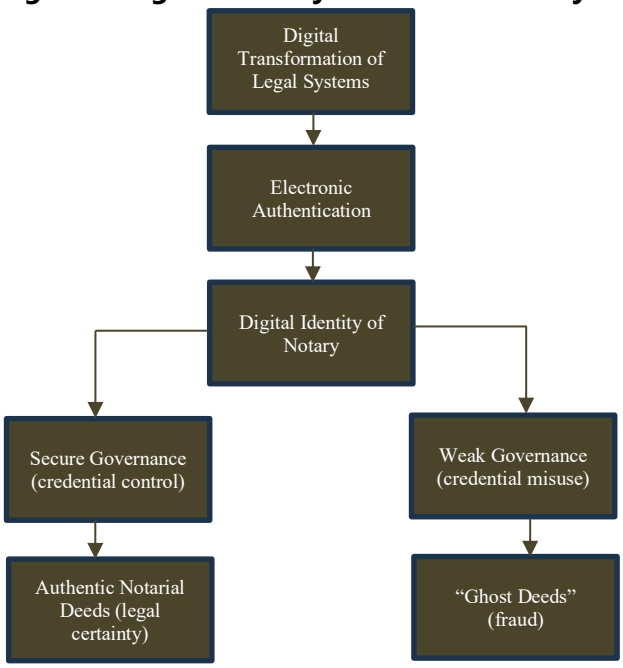
From a regulatory standpoint, the transformation of authentication mechanisms requires a reassessment of institutional safeguards. Legal systems must ensure that digital infrastructures preserve the same level of reliability traditionally associated with physical verification. This includes mechanisms for identity control, credential management, and continuous oversight of digital authentication systems. Without such safeguards, the presumption of authenticity attached to notarial deeds may gradually lose its normative foundation.

In the absence of adequate safeguards, the risks associated with digital identity misuse may evolve into systemic threats affecting the integrity of legal transactions. The potential circulation of ghost deeds undermines confidence in authentic documents and introduces uncertainty into legal relationships that rely on notarial certification. This uncertainty may ultimately weaken the trust that underpins property systems, commercial transactions, and contractual enforcement.

For these reasons, the phenomenon of cyber risks in notarial practice should not be understood merely as a technological problem. Rather, it reflects a structural challenge arising from the intersection of legal authority and digital governance. Addressing this challenge requires the development of regulatory frameworks capable of integrating technological safeguards with established legal principles. Only through such integration can modern legal systems preserve the authenticity and reliability that form the cornerstone of notarial institutions.

[21] Ulrich Beck, *Risk Society: Towards a New Modernity* (London: Sage Publications, 1992), 19–23.

Figure I. Digital Identity Risk in Notarial Systems



As Figure 1 illustrates the relationship between digital transformation and the risks associated with digital identity in notarial systems. The diagram demonstrates that the digitalization of legal services introduces electronic authentication mechanisms that rely on digital identity credentials. When these credentials are governed through secure oversight mechanisms, the system can maintain the reliability and authenticity traditionally associated with notarial deeds. However, when governance mechanisms fail, particularly in situations where digital identities remain active after the death of a notary, the same technological infrastructure may facilitate the creation of unauthorized documents. These documents, referred to as "ghost deeds," represent a critical point where technological vulnerability intersects with legal authority, thereby undermining legal certainty and institutional trust.

3.2. Legal Vacuum in Post-Mortem Identity and Access Control

The effectiveness and legitimacy of digital transformation in notarial practice do not depend solely on technological innovation or the formal recognition of electronic systems, but also on the presence of structured regulatory safeguards capable of ensuring legal certainty, authenticity, security, and accountability. In the Indonesian context, the legal framework governing notarial authority, electronic transactions, and digital authentication has developed through the Law on Notarial Office, the Law on Electronic Information and Transactions, and related regulations on electronic systems and certification. However, these regulatory regimes remain insufficiently integrated in addressing the legal consequences that arise when a notary's authority terminates while the digital credentials associated with that professional identity remain technically functional. This regulatory disjunction creates a normative vulnerability in which electronic certificates, authentication credentials, or other forms of digital identity may potentially continue to be used after the legal authority to which they were originally attached has ceased. Rather than constituting a merely technical cybersecurity

problem, such circumstances raise fundamental questions concerning the authenticity of notarial acts, defects of authority, evidentiary reliability, and institutional responsibility. It is therefore necessary to critically examine whether the existing regulatory framework provides adequate mechanisms for the immediate termination, revocation, and supervision of notarial digital credentials following death or other forms of cessation of office, and how the absence of such mechanisms may undermine the principles of legal certainty and public trust in authentic instruments.

The digitalization of notarial administration has fundamentally altered the institutional architecture through which legal authority is exercised. While the classical doctrine of notarial authority assumes that the competence of a notary ceases immediately upon death, digital infrastructures do not necessarily reflect this juridical termination. In traditional systems, the authority of the notary is inseparable from the person of the office holder, and therefore the death of the notary automatically extinguishes the capacity to produce authentic deeds[22]. However, the persistence of digital identities within electronic authentication systems reveals a critical normative inconsistency: technological systems may continue to recognize an identity even after the legal authority attached to that identity has ceased to exist.

This discrepancy exposes what may be described as a post-mortem authority paradox within contemporary notarial governance. On the one hand, the legal system recognizes that a deceased notary cannot exercise professional authority. On the other hand, digital authentication infrastructures may continue to validate credentials associated with that same individual. In such circumstances, the technological infrastructure effectively preserves a functional representation of authority that the legal system has already terminated. This paradox illustrates a structural regulatory gap in the governance of digital identity within notarial systems.

The Indonesian Law on Notarial Office reflects a regulatory model rooted in the logic of physical documentation. The law meticulously regulates the custody and transfer of notarial protocols after a notary ceases to hold office, ensuring that archives remain preserved within the institutional framework of legal administration[23]. Yet this regulatory structure presupposes that the instruments of notarial authority are physical documents rather than digital credentials. Consequently, the law provides no explicit mechanism for addressing the continuation of electronic identities associated with notarial authority. This silence within the regulatory framework is not merely an omission but constitutes a substantive normative deficiency. Digital identity has become the functional equivalent of institutional authority in modern administrative systems. Electronic certificates, authentication credentials, and digital access tokens effectively operate as gateways through which professional authority is exercised within digital platforms[24]. If such credentials remain active beyond the life of the

[22] J.H. Merryman and Rogelio Pérez-Perdomo, The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America, 3rd ed. (Stanford: Stanford University Press, 2007), 114–116.
[23] See Law No. 30 of 2004 concerning the Notarial Office, arts. 1 point 13 and 62; Law No. 2 of 2014 concerning Amendment to Law No. 30 of 2004 concerning the Notarial Office, art. 63(1)–(6); see also art. 16(1)(b).
[24] Daniel J. Solove, Understanding Privacy (Cambridge, MA: Harvard University Press, 2008), 98–100.

notary, the system creates a technological continuation of authority that contradicts the legal termination of office.

The absence of explicit regulatory provisions concerning the termination of digital authority therefore produces a doctrinal gap within the legal structure of notarial governance. The existing framework assumes that the termination of professional authority automatically eliminates the capacity to exercise that authority. However, in digital environments, authority is mediated through technological credentials that may persist independently of the individual who originally possessed them. This disjunction reveals that the law has not yet fully internalized the implications of digital identity within the institutional design of notarial authority.

Another dimension of this normative gap concerns the absence of mechanisms for automatic revocation of authentication credentials. Digital identity systems typically rely on certification authorities that issue and validate electronic credentials through cryptographic infrastructure. Such systems operate on the assumption that credentials remain valid until they are formally revoked[25]. When the death of a notary does not trigger automatic revocation procedures, the authentication infrastructure continues to recognize the credentials as legitimate. This technological persistence creates a legal anomaly in which the authentication system may validate actions that lack any lawful authority. Furthermore, the regulatory framework does not adequately address the governance of digital protocols. While the law provides detailed rules regarding the transfer of physical notarial archives, it remains silent concerning the management of digital records, authentication devices, and electronic access credentials. The concept of "notarial protocol" has historically been interpreted as referring to physical documentation, yet the digital transformation of legal administration suggests that protocols now include electronic components that require separate regulatory treatment.

This conceptual gap becomes particularly significant when considering the evidentiary implications of documents generated through compromised digital identities. Authentic deeds traditionally derive their evidentiary authority from the presumption that they are produced by a legally authorized official acting within the scope of his or her competence. If digital systems permit the continued use of credentials associated with deceased notaries, this presumption becomes structurally unstable. The authenticity of a document may then be simulated through technological means even though the underlying authority no longer exists. The legal consequences of this phenomenon extend beyond isolated cases of fraud. The persistence of digital authority after death introduces a systemic vulnerability within the architecture of legal authentication. Documents generated through unauthorized digital identities may circulate within administrative systems, financial institutions, and judicial proceedings before their irregular origins are discovered. Such circumstances threaten the reliability of authentic deeds as instruments of legal certainty.

From a doctrinal standpoint, the emergence of post-mortem digital identity misuse requires a re-evaluation of the relationship between professional authority and technological

[25] Bart van Looy et al., "Digital Identity and Legal Authentication," Computer Law & Security Review 37 (2020): 5–7.

infrastructure. The traditional legal assumption that authority is inseparable from the individual office holder no longer holds true in digital environments where identity can be technologically replicated or preserved. This transformation suggests the need for a new regulatory concept that explicitly addresses the governance of digital authority after the termination of professional office. This article therefore introduces the concept of post-mortem notarial identity governance as a normative framework for addressing these challenges. The concept emphasizes that the termination of professional authority must be accompanied by the simultaneous termination of all digital credentials associated with that authority. Without such synchronization between legal authority and technological systems, the digital infrastructure of notarial administration will remain vulnerable to exploitation.

In this sense, the phenomenon of ghost deeds should not be understood merely as an instance of technological misuse but as a manifestation of a deeper regulatory failure. The legal system has successfully developed elaborate mechanisms for safeguarding physical documents, yet it has not established equivalent safeguards for digital authority. Addressing this imbalance requires a comprehensive regulatory approach capable of integrating technological governance into the doctrinal structure of notarial law.

To see in a broader standpoint, Table 1 below demonstrates that the current regulatory framework governing notarial practice remains primarily oriented toward physical documentation. While the law provides detailed mechanisms for managing physical protocols and administrative responsibilities, it does not adequately address the governance of digital identities and authentication systems. This normative gap creates systemic vulnerabilities that may allow digital credentials to remain active even after the termination of professional authority.

Table 1. Normative Gaps in Post-Mortem Notarial Identity GovernanceB

(*Secondary Data, Processed 2026*)#

Regulatory Dimension	Existing Regulation	Identified Gap	Legal Risk
Termination of Notarial Authority	Regulated upon death of notary	No digital identity termination mechanism	Persistence of digital authority
Notarial Protocol	Transfer of physical archives regulated	Digital protocols not regulated	Unauthorized digital document access
Authentication Credentials	Electronic certificates recognized	No automatic revocation after death	Misuse of authentication systems
Supervisory Mechanism	Professional supervision exists	No cybersecurity oversight	Undetected identity misuse

Source: Author's analysis based on Law Number 30 of 2004 concerning the Office of Notary as amended by Law Number 2 of 2014; Law Number 11 of 2008 concerning Electronic

Information and Transactions as last amended by Law Number 1 of 2024; Regulation of the Minister of Law and Human Rights Number 15 of 2020 concerning Procedures for Notarial Supervisory Council Examinations; and Regulation of the Minister of Law and Human Rights Number 16 of 2021 concerning the Organization and Governance of the Notarial Supervisory Council.

3.3. Post-Mortem Digital Authority and the Legal Status of Ghost Deeds

The phenomenon of ghost deeds exposes a deeper conceptual problem that extends beyond cybersecurity vulnerabilities and regulatory deficiencies. At its core, the issue challenges the traditional understanding of authority within notarial law. Classical notarial doctrine is built upon the assumption that legal authority is inseparable from the person of the office holder. A notary derives authority directly from statutory delegation and exercises that authority personally through acts of authentication, verification, and legal formalization. Consequently, the death of a notary automatically extinguishes the authority attached to that office. However, digital environments increasingly complicate this assumption because elements of professional identity may continue to exist and operate independently from the individual who originally possessed them.[26]

The growing reliance on digital infrastructures has transformed the manner in which professional authority is exercised. Contemporary notarial systems increasingly depend on digital certificates, authentication credentials, electronic signatures, and interconnected governmental databases. These technologies do not merely facilitate administrative efficiency; they have become integral to the exercise of legal authority itself. In practical terms, access to digital systems determines whether a notary can perform authentication functions, interact with public registries, and generate legally recognized documentation. As a result, authority is no longer exercised solely through physical office but increasingly through digital infrastructures.[27]

This transformation has significant theoretical implications. Traditionally, legal identity and legal authority were treated as distinct concepts. Identity served merely as a mechanism for identifying the person entitled to exercise authority. In digital environments, however, identity increasingly functions as the operational mechanism through which authority is exercised. The possession of valid digital credentials effectively enables participation in legal processes and access to institutional powers. Consequently, digital identity has evolved from a passive identifier into an active component of legal authority itself.[28]

The persistence of digital identity following the death of a notary therefore creates a unique legal anomaly. While the law recognizes that professional authority ceases upon death, digital systems may continue to recognize the credentials associated with the deceased

[26] Bart van Looy et al., "Digital Identity and Legal Authentication," *Computer Law & Security Review* 37 (2020): 5–8, https://doi.org/10.1016/j.clsr.2020.105430.
[27] Michael Veale and Frederik Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act," *Computer Law Review International* 22, no. 4 (2021): 97–112, https://doi.org/10.9785/cri-2021-220402.
[28] Karen Yeung and Martin Lodge, "Algorithmic Regulation and Accountability," *Regulation & Governance* 16, no. 3 (2022): 629–644, https://doi.org/10.1111/rego.12406.

individual as valid. This creates a divergence between legal reality and technological reality. Legally, the authority no longer exists. Technologically, however, the infrastructure may continue to facilitate actions that outwardly appear to originate from a legally authorized official. Such divergence generates conditions under which unauthorized actors may exploit digital identities to produce documents that appear formally authentic.

This discrepancy demonstrates that digital authority possesses characteristics that differ fundamentally from traditional legal authority. Conventional authority terminates automatically upon the occurrence of legally recognized events, such as death, resignation, or dismissal. Digital authority, by contrast, may persist indefinitely unless technological systems are specifically designed to revoke access and authentication credentials. The existence of such persistence suggests that digital systems create a secondary layer of authority that is not fully governed by existing legal doctrines.[29]

The emergence of this phenomenon necessitates the development of a new conceptual framework. This article introduces the concept of Post-Mortem Digital Authority (PMDA) to describe situations in which technological systems continue to recognize and operationalize digital representations of professional authority after the legal termination of office. PMDA does not imply the lawful continuation of authority. Rather, it refers to a condition in which technological infrastructures fail to synchronize with legal reality, thereby enabling unauthorized exercises of apparent authority. The concept provides a theoretical explanation for why ghost deeds continue to emerge despite the formal termination of notarial authority.

The concept of PMDA is particularly relevant within the context of public authentication systems. Unlike ordinary digital accounts, notarial credentials are linked to state-recognized authority and carry significant legal consequences. Their misuse may affect property rights, contractual relations, corporate governance, and judicial proceedings. Consequently, the persistence of digital credentials after death should not be viewed merely as a cybersecurity issue. Instead, it constitutes a governance problem involving the improper continuation of state-delegated authority within digital environments.[30]

From a jurisprudential perspective, PMDA also challenges the traditional relationship between authority and responsibility. Legal systems generally presume that authority and accountability are inseparable. A public official who exercises authority can be identified, supervised, and held responsible for the consequences of his or her actions. Ghost deeds disrupt this relationship by creating situations in which apparent authority exists without a corresponding legal subject capable of assuming responsibility. This undermines one of the foundational principles underlying public administration and professional regulation.

The phenomenon further demonstrates that the doctrine of legal personality has not yet been fully adapted to digital governance. Existing legal frameworks regulate the termination of professional authority through administrative procedures, yet they rarely address the

[29] Luciano Floridi, "The Ontological Interpretation of Informational Privacy," *Ethics and Information Technology* 24, no. 3 (2022): 1–11, https://doi.org/10.1007/s10676-022-09621-2.
[30] David Birch, "Digital Identity and the Future of Trust," *Computer Law & Security Review* 47 (2022): 105725, https://doi.org/10.1016/j.clsr.2022.105725.

technological afterlife of digital identities. As digital infrastructures become increasingly central to legal administration, the failure to regulate post-mortem digital identity may create systemic vulnerabilities capable of undermining public trust in legal institutions.[31]

The emergence of PMDA also reveals the limitations of current approaches to digital identity governance. Most regulatory frameworks focus on identity verification, authentication reliability, and cybersecurity protection. While these concerns remain important, they do not address the broader question of what happens when legal authority ceases but digital credentials remain active. The absence of legal mechanisms governing post-mortem digital identity leaves a critical gap between technological operation and legal doctrine.

PMDA differs from existing theories of digital identity governance because its principal concern is not merely the management, authentication, security, or revocation of digital credentials. Conventional digital identity governance primarily focuses on ensuring that digital identities are reliably verified, securely managed, and appropriately deactivated throughout their lifecycle. PMDA addresses a narrower but distinct legal condition in which the underlying legal authority has already terminated, while the digital credentials representing that authority remain technically recognizable or usable. Its conceptual focus therefore lies in the divergence between the legal lifecycle of public authority and the technological lifecycle of the credentials through which that authority is exercised. In the notarial context, PMDA arises where a notary previously possessed legally conferred authority, that authority terminates by operation of law, the associated digital credentials remain technically functional, and such persistence enables an act to appear as though it originated from a legally authorized notary.[32]

This distinction also affects the legal characterization of ghost deeds. Under Article 8 paragraph (1) letter a of Law Number 30 of 2004 concerning the Office of Notary, notarial authority terminates upon the death of the notary. Accordingly, the continued technical functionality of a deceased notary's digital credentials cannot revive or extend that authority. A deed produced through the post-mortem use of such credentials therefore cannot acquire the status of an authentic deed because Article 1868 of the Indonesian Civil Code requires an authentic deed to be made by or before a legally competent public official. Nevertheless, the loss of authentic character should not automatically be equated with the nullity of every underlying legal transaction. Article 1869 of the Civil Code recognizes that an instrument which fails to qualify as an authentic deed because of the incompetence or lack of authority of the public official may, under certain conditions, retain evidentiary value as a private instrument. The legal consequences of a ghost deed must therefore be assessed by distinguishing between the authenticity of the deed, the validity of the underlying transaction, and the formal requirements applicable to that particular legal act.

The position of good-faith third parties requires a separate assessment. Good faith

[31] European Union Agency for Cybersecurity (ENISA), *Trust Services and Digital Identity in Europe: Threat Landscape Report* (Athens: ENISA, 2023), 22–29; lihat juga World Bank, *Digital Identity for Inclusive and Trusted Public Services* (Washington, DC: World Bank, 2024), 33–41.

[32] David Temoshok et al., NIST SP 800-63-4: Digital Identity Guidelines (Gaithersburg, MD: National Institute of Standards and Technology, 2025), https://doi.org/10.6028/NIST.SP.800-63-4.

cannot restore notarial authority that has already ceased, nor can it convert a ghost deed into an authentic instrument. However, the interests of third parties who reasonably relied on the apparent validity of a transaction may still deserve protection where the applicable legal requirements are satisfied. Such protection should depend on factors including whether the third party followed legally prescribed procedures, exercised reasonable due diligence, and had no reasonable means of detecting the defect in the notary's authority. Accordingly, the appropriate legal conclusion is not that every ghost deed and every transaction connected to it are automatically null and void, but that the deed itself cannot possess authentic notarial character, while the validity of the underlying transaction and the protection of subsequent good-faith third parties must be determined separately according to the applicable rules of private law.

Accordingly, digital identity should no longer be understood solely as a technical instrument of authentication. In contemporary legal systems, digital identity increasingly functions as an extension of public authority. This transformation requires a corresponding evolution in legal regulation. If authority is exercised through digital credentials, then the termination of authority must necessarily include the termination of those credentials. Failure to achieve such synchronization will continue to generate opportunities for unauthorized exercises of apparent authority.

Ultimately, the concept of Post-Mortem Digital Authority provides a theoretical foundation for understanding ghost deeds as manifestations of a broader governance failure rather than isolated incidents of fraud. The persistence of digital authority beyond the life of its lawful holder illustrates the growing tension between legal institutions designed for an analog era and technological infrastructures operating in digital environments. Recognizing and regulating this phenomenon is therefore essential for preserving legal certainty, protecting public trust, and ensuring that technological systems remain subordinate to the principles governing lawful authority.

The emergence of ghost deeds raises fundamental doctrinal questions concerning the legal validity of documents produced through the unauthorized use of a deceased notary's digital identity. In civil law jurisdictions, the authenticity of a notarial deed is not merely a matter of formal documentation but is intrinsically linked to the authority of the notary as a public official empowered by the state to formalize legal acts. The legal force of an authentic deed therefore derives from the institutional authority vested in the notary rather than from the document itself[33]. When that authority ceases, the legal foundation upon which authentic deeds are produced necessarily disappears.

3.4. Legal Validity and Liability of Ghost Deeds

The emergence of ghost deeds raises fundamental doctrinal questions concerning the legal validity of documents produced through the unauthorized use of a deceased notary's digital identity. In civil law jurisdictions, the authenticity of a notarial deed is not merely a

[33] J.H. Merryman and Rogelio Pérez-Perdomo, The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America, 3rd ed. (Stanford: Stanford University Press, 2007), 112–114.

matter of formal documentation but is intrinsically linked to the authority of the notary as a public official empowered by the state to formalize legal acts. The legal force of an authentic deed therefore derives from the institutional authority vested in the notary rather than from the document itself[34]. When that authority ceases, the legal foundation upon which authentic deeds are produced necessarily disappears.

Within the doctrinal framework of notarial law, the authority of a notary is inseparable from the person holding the office. The competence to produce authentic deeds is granted by law and exercised personally by the notary in the performance of public duties. Consequently, the death of a notary automatically terminates the legal competence required to produce authentic deeds. This termination represents not merely an administrative event but a juridical cessation of authority recognized by the legal system.[35] Any document generated after such termination therefore lacks the institutional legitimacy required to be recognized as an authentic deed.

However, the digitalization of administrative systems introduces a new dimension to this doctrinal structure. Electronic authentication systems such as digital certificates, login credentials, and cryptographic keys, may continue to exist within digital infrastructures even after the legal authority of the notary has ceased. In practical terms, digital platforms may still recognize the electronic credentials associated with a deceased notary as valid authentication tools. This technological persistence creates the possibility that documents may be generated using credentials belonging to individuals who no longer possess legal authority.

This phenomenon reveals a fundamental discrepancy between technological identity recognition and juridical authority recognition. While digital systems authenticate identity through technical credentials, legal systems recognize authority only when exercised by a competent public official acting within the scope of his or her lawful authority. The coexistence of these two distinct mechanisms creates the structural conditions under which ghost deeds may emerge. From a doctrinal standpoint, the central legal issue concerns whether documents generated through such unauthorized digital identities can still be regarded as authentic deeds. Authentic deeds derive their evidentiary authority from the presumption that they are produced by a legally authorized notary performing a public function.[36] When such authority is absent, the essential condition required for the authenticity of the deed is not fulfilled.

This distinction highlights the difference between formal authenticity and juridical authenticity. Ghost deeds may appear formally authentic because they reproduce the structural features of legitimate deeds, including digital signatures, formatting, and authentication markers. However, juridical authenticity depends upon the lawful exercise of authority by a competent public official. When such authority is absent, the document cannot acquire the legal status of an authentic deed regardless of its outward appearance.

---

[34] J.H. Merryman and Rogelio Pérez-Perdomo, The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America, 3rd ed. (Stanford: Stanford University Press, 2007), 112–114.

[35] Lawrence M. Friedman, The Legal System: A Social Science Perspective (New York: Russell Sage Foundation, 1975), 15–18.

[36] Peter Mahmud Marzuki, Penelitian Hukum, rev. ed. (Jakarta: Kencana, 2017), 92–93.

In doctrinal terms, the defect underlying ghost deeds can be characterized as a defect of authority (*defectus potestatis*). This type of defect differs fundamentally from procedural irregularities that may render a deed voidable. Instead, the absence of lawful authority strikes at the very foundation of the deed's authenticity. Under classical principles of notarial law, a document produced without lawful authority cannot acquire the legal status of an authentic deed.

Accordingly, ghost deeds should be classified as null and void ab initio. The defect arises at the moment of creation because the document is produced without the participation of a legally authorized public official. Consequently, such documents never acquire the evidentiary privileges normally attached to authentic deeds.[37] Courts confronted with ghost deeds should therefore treat them not as defective authentic deeds but as instruments that never possessed authentic status. The evidentiary implications of this classification are significant. Authentic deeds traditionally possess strong probative force and may constitute conclusive evidence regarding the statements contained therein. If a document is produced without lawful authority, this evidentiary presumption collapses. The document may still be examined as a private instrument or factual record, but it cannot enjoy the privileged evidentiary status associated with authentic deeds.

The circulation of ghost deeds also raises complex questions concerning the protection of third parties acting in good faith. Legal systems often seek to protect innocent parties who rely upon authentic documents in commercial transactions. However, extending such protection to documents produced without lawful authority would create doctrinal inconsistencies. The principle of good faith cannot legitimize acts that were never legally valid in the first place.[38] At this stage, it becomes necessary to examine the broader framework of legal responsibility arising from the misuse of a deceased notary's identity. The phenomenon of ghost deeds does not merely affect the validity of documents but also raises questions concerning administrative accountability, civil liability, and criminal responsibility. These dimensions of liability are interconnected and may arise simultaneously within the legal system.

[37] Terry Hutchinson, Researching and Writing in Law, 3rd ed. (Sydney: Thomson Reuters, 2018), 9–11.
[38] Roger Brownsword, Law, Technology and Society (Abingdon: Routledge, 2019), 41–43.

Figure 2. Multi-Layer Liability Structure of Ghost Deeds

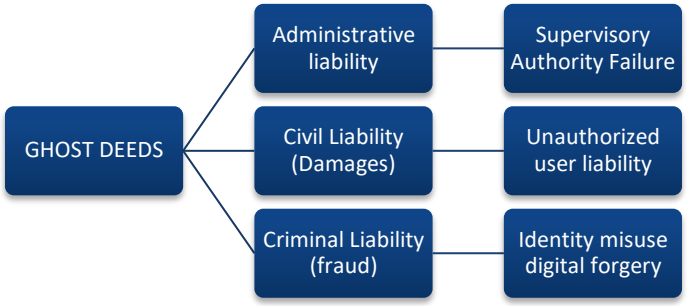


Figure 2 illustrates the multi-layer structure of legal responsibility that may arise from the misuse of a deceased notary's digital identity. The diagram demonstrates that liability may emerge simultaneously within administrative, civil, and criminal law frameworks. Administrative liability may arise from failures of institutional supervision, particularly where regulatory authorities do not establish mechanisms for terminating digital credentials following the death of a notary. Civil liability may arise when parties suffer financial losses as a result of transactions based on ghost deeds. Criminal liability may apply when individuals intentionally exploit digital credentials to produce fraudulent documents or conduct unlawful transactions.

From an administrative perspective, supervisory institutions responsible for regulating the notarial profession may bear responsibility if regulatory mechanisms fail to ensure the timely deactivation of digital credentials associated with notarial authority. Inadequate oversight of authentication systems may contribute to circumstances in which digital identities remain active even after the termination of professional authority. On the other hand, civil liability may arise when ghost deeds cause financial harm to parties who rely on their apparent authenticity. Individuals who intentionally access or exploit digital credentials belonging to deceased notaries may be required to compensate victims for losses arising from fraudulent transactions. Such liability may also extend to parties who negligently fail to secure authentication systems under their control.

3.5. Toward a Cyber Governance Model for Notarial Systems

The emergence of ghost deeds demonstrates that the regulatory framework governing notarial practice has not evolved at the same pace as the digital infrastructures through which notarial functions are increasingly performed. Traditional notarial law was developed within an analog administrative environment in which authority and identity were inseparable. However, contemporary legal transactions increasingly rely on electronic authentication systems, digital signatures, and interconnected governmental databases. This transformation requires a regulatory framework capable of ensuring that technological infrastructures accurately reflect the legal principles governing professional authority.[39]

[39] Roger Brownsword, Law, Technology and Society (London: Routledge, 2019), 73–75.

The persistence of digital credentials associated with deceased notaries illustrates a fundamental governance gap between legal authority and technological control. Existing legal frameworks primarily regulate the termination of notarial authority through administrative mechanisms, such as the transfer of physical protocols and the appointment of custodians for notarial archives. Yet these mechanisms do not address the management of digital identities embedded within electronic authentication systems. As a result, technological infrastructures may continue to recognize digital identities belonging to individuals who no longer possess legal authority.

This regulatory gap reveals the limitations of traditional legal doctrines when confronted with technologically mediated authentication systems. Legal rules governing the termination of notarial authority assume that professional identity ceases simultaneously with the termination of office. Digital infrastructures, however, operate according to technical protocols that may allow credentials to persist indefinitely unless actively revoked. This mismatch between legal termination and technological persistence creates the structural conditions under which ghost deeds may emerge.

Addressing this problem requires more than incremental regulatory adjustments. Instead, it necessitates the development of an integrated cyber governance framework capable of synchronizing legal authority with technological authentication systems. Such a framework must ensure that the termination of notarial authority is automatically reflected within digital infrastructures that control authentication processes.

The cyber governance model proposed in this study seeks to establish such synchronization by introducing a regulatory architecture that integrates civil registry systems, authentication infrastructures, and supervisory institutions. The objective of this model is to ensure that digital identities associated with notarial authority cannot persist beyond the lawful duration of professional office

Figure 3. Proposed Cyber Governance Model for Notarial Systems

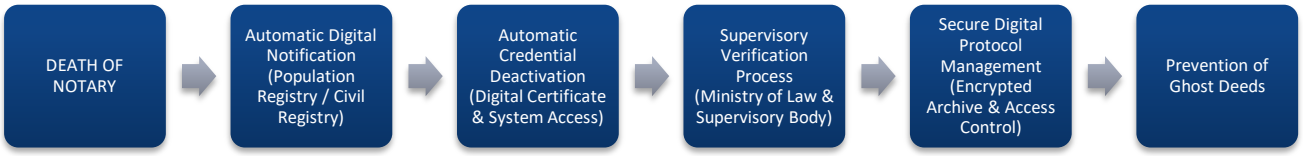


Figure 3 illustrates the proposed governance architecture designed to prevent the persistence of digital identities beyond the termination of notarial authority. The model emphasizes the need for an automated mechanism that connects civil registry databases with authentication systems used within notarial administration. When the death of a notary is officially recorded, the system should automatically initiate the deactivation of digital credentials associated with that individual.

The first pillar of this model is automatic digital deactivation of professional credentials. Digital certificates, authentication tokens, and system access rights associated with the notary must be immediately revoked once the termination of authority is registered within official

databases. This mechanism ensures that digital infrastructures cannot continue to recognize the identity of a deceased notary as a valid authentication authority. The second pillar involves the establishment of strict digital identity certification standards for notarial professionals. Digital identities associated with notarial authority should be governed by high-level security protocols similar to those used in financial institutions and governmental authentication systems. These protocols should incorporate encryption standards, multi-factor authentication, and centralized verification mechanisms capable of preventing unauthorized access to professional credentials[40].

Next, the third pillar of the proposed model concerns the implementation of mandatory cybersecurity and compliance audits within notarial authentication systems. Regular security audits would enable supervisory institutions to evaluate whether authentication infrastructures comply with regulatory standards governing digital identity management. Such audits would also allow authorities to detect vulnerabilities that may permit unauthorized access to digital credentials. Furthermore, the fourth pillar proposes the adoption of advanced authentication technologies, including blockchain-based verification mechanisms. Distributed ledger technologies can provide transparent and tamper-resistant records of authentication processes. By recording authentication events within immutable digital ledgers, blockchain infrastructures may enhance the integrity of notarial authentication systems and significantly reduce the possibility of unauthorized document creation[41].

The fifth pillar concerns the establishment of a clear liability framework governing digital authentication within notarial systems. The misuse of digital credentials belonging to deceased notaries must be accompanied by clearly defined legal consequences for individuals or institutions responsible for such misuse. A well-defined liability framework would strengthen deterrence and promote greater accountability within digital authentication infrastructures. In addition, supervisory institutions responsible for regulating the notarial profession must expand their role to include cybersecurity oversight within digital authentication systems. Professional regulation can no longer focus solely on traditional administrative supervision. Instead, regulatory authorities must develop institutional capacities capable of monitoring technological infrastructures that support the production of authentic deeds.

Finally, addressing the phenomenon of ghost deeds may require targeted reforms within criminal law frameworks. Existing provisions governing forgery and identity fraud may not adequately capture the unique risks associated with the digital misuse of professional identities. Introducing specific criminal provisions addressing unauthorized use of digital credentials within public authentication systems would strengthen the legal framework governing digital misconduct in notarial practice. In conclusion, the cyber governance framework proposed in this study aims to ensure that digital authentication infrastructures

[40] Mireille Hildebrandt, Smart Technologies and the End(s) of Law (Cheltenham: Edward Elgar, 2015), 102–104.
[41] Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code (Cambridge: Harvard University Press, 2018), 41–45.

remain consistent with the legal principles governing notarial authority. By synchronizing technological systems with the juridical termination of professional office, the proposed model seeks to prevent the persistence of digital identities beyond the lawful duration of their holders. In doing so, the framework contributes to preserving the institutional reliability of authentic deeds while simultaneously adapting notarial regulation to the realities of digital transformation.

The feasibility of this model does not necessarily require the creation of an entirely new centralized database. Rather, it can be developed through event-based interoperability among existing institutional systems. At present, the Directorate General of Population and Civil Registration (Dukcapil) maintains population and civil-registration data, while the Directorate General of General Legal Administration (Ditjen AHU) administers the appointment, status, and termination of notarial office through its electronic system. Existing administrative practice already requires the death of a notary to be reported to Ditjen AHU, accompanied by a legalized death certificate, before a formal decision on termination is issued. The proposed model would reduce dependence on this manual notification by allowing an officially registered death event in the population database to generate a limited electronic notification to the notarial administration system. Such interoperability is institutionally plausible because Indonesian law already provides a framework for authorized access to and utilization of population data under Minister of Home Affairs Regulation Number 102 of 2019, as amended by Minister of Home Affairs Regulation Number 17 of 2023.

The proposed sequence would operate in several stages. First, once a notary's death is formally recorded in the population administration system, Dukcapil would transmit a verified status notification containing only the information necessary to identify the relevant notary. Second, Ditjen AHU would match that notification with the notarial registry and change the professional status of the notary to a provisional inactive status pending administrative verification. Third, the change of status would trigger notification to the relevant Electronic Certification Provider (PSrE) for immediate blocking and subsequent revocation of electronic certificates and authentication credentials associated with the deceased notary. Fourth, the revocation status would be published through existing certificate-validation mechanisms, including the Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL), so that connected systems could no longer accept the credential as valid. Finally, the relevant Notarial Supervisory Council should be notified to supervise the transfer of the notarial protocol and other post-office administrative obligations. To prevent erroneous deactivation, the model should incorporate auditable logs, institutional verification, and an exception procedure for disputed or incorrectly matched records. Inter-agency data exchange should also follow the principles of purpose limitation and data minimization, so that the system communicates a verified change of legal status rather than transferring unnecessary population data.

4. CONCLUSION

The phenomenon of ghost deeds reveals a structural tension between traditional

doctrines of notarial authority and the realities of digital authentication systems. This study demonstrates that the unauthorized use of a deceased notary's digital identity undermines the foundational principle that the authenticity of a notarial deed derives from the lawful authority of a living public official. From a doctrinal perspective, documents produced under such circumstances must be regarded as null and void ab initio due to a fundamental defect of authority, thereby depriving them of the evidentiary privileges associated with authentic deeds. At the same time, the persistence of digital credentials after the termination of professional authority exposes significant regulatory gaps within existing legal frameworks governing notarial practice. Addressing this problem therefore requires more than doctrinal clarification; it demands the development of an integrated cyber governance framework capable of synchronizing legal authority with digital authentication infrastructures. The model proposed in this study offers a normative pathway for preventing the emergence of ghost deeds while preserving the institutional reliability of authentic deeds in an increasingly digital legal environment.

REFERENCE

Alkatiri, Naurah Humam, Mohamad Fajri Mekka Putra, and Kyle Ongko. "A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era." Jambura Law Review 5, no. 2 (2023): 332–55. https://doi.org/10.33756/jlr.v5i2.19221.

Beck, Ulrich. Risk Society: Towards a New Modernity. London: Sage, 1992.

Birch, David. "Digital Identity and the Future of Trust." Computer Law & Security Review 47 (2022): 105725. https://doi.org/10.1016/j.clsr.2022.105725.

Brownsword, Roger, Eloise Scotford, and Karen Yeung, eds. The Oxford Handbook of Law, Regulation and Technology. Oxford: Oxford University Press, 2017.

Brownsword, Roger. Law, Technology and Society. Abingdon: Routledge, 2019.

Calo, Ryan. "Artificial Intelligence Policy: A Primer and Roadmap." UC Davis Law Review 51, no. 2 (2017): 399–435.

Cohen, Julie E. Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford: Oxford University Press, 2019.

Cunneen, Máirtín, Ruhi AnandFinn, Raymond Friel, Paul Tennent, and Sami Brandt. "From Bones to Bytes: Anticipating and Addressing the Governance Challenges of Human Digital Remains and Posthumous Digital Human Twins." AI & Society 41 (2026): 2021–40. https://doi.org/10.1007/s00146-025-02514-4.

De Filippi, Primavera, and Aaron Wright. Blockchain and the Law: The Rule of Code. Cambridge, MA: Harvard University Press, 2018.

European Union Agency for Cybersecurity. Trust Services and Digital Identity in Europe: Threat Landscape Report. Athens: ENISA, 2023.

Financial Action Task Force. Guidance for a Risk-Based Approach to Legal Professionals. Paris: FATF, 2019.

Floridi, Luciano. "The Ontological Interpretation of Informational Privacy." Ethics and Information Technology 24, no. 3 (2022): 1–11. https://doi.org/10.1007/s10676-022-09621-2.

Friedman, Lawrence M. The Legal System: A Social Science Perspective. New York: Russell Sage Foundation, 1975.

Hildebrandt, Mireille, and Katja de Vries, eds. Privacy, Due Process and the Computational Turn. London: Routledge, 2013.

Hildebrandt, Mireille. Smart Technologies and the End(s) of Law. Cheltenham: Edward Elgar, 2015.

Hollanek, Tomasz, and Katarzyna Nowaczyk-Basińska. "Griefbots, Deadbots, Postmortem Avatars: On Responsible Applications of Generative AI in the Digital Afterlife Industry." Philosophy & Technology 37, no. 2 (2024): Article 63. https://doi.org/10.1007/s13347-024-00744-w.

Hutchinson, Terry. Researching and Writing in Law. 3rd ed. Sydney: Thomson Reuters, 2018.

Ibrahim, Johnny. Teori dan Metodologi Penelitian Hukum Normatif. Malang: Bayumedia, 2006.

Koops, Bert-Jaap. "The Concept of Identity in Digital Legal Systems." Computer Law & Security Review 32, no. 5 (2016): 724–35.

Lessig, Lawrence. Code and Other Laws of Cyberspace. New York: Basic Books, 2006.

Marzuki, Peter Mahmud. Penelitian Hukum. Rev. ed. Jakarta: Kencana, 2017.

Merryman, John Henry, and Rogelio Pérez-Perdomo. The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America. 3rd ed. Stanford, CA: Stanford University Press, 2007.

Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press, 2010.

Reidenberg, Joel R. "Lex Informatica: The Formulation of Information Policy Rules through Technology." Texas Law Review 76, no. 3 (1998): 553–84.

Republic of Indonesia. Law No. 30 of 2004 concerning Notarial Office, as Amended by Law No. 2 of 2014.

Robles-Carrillo, Margarita. "Digital Identity: An Approach to Its Nature, Concept, and Functionalities." International Journal of Law and Information Technology 32 (2024): eaae019. https://doi.org/10.1093/ijlit/eaae019.

Solove, Daniel J. Understanding Privacy. Cambridge, MA: Harvard University Press, 2008.

Solove, Daniel J., and Paul M. Schwartz. Information Privacy Law. New York: Aspen Publishers, 2020.

Toruan, Henry Donald Lbn. "The Importance of Using Electronic Deeds to Facilitate the Service and Storage of Notary Archives." Jurnal Penelitian Hukum De Jure 22, no. 4 (2022): 483–98. https://doi.org/10.30641/dejure.2022.V22.483-498.

Van Looy, Bart, et al. "Digital Identity and Legal Authentication." Computer Law & Security Review 37 (2020): 105430. https://doi.org/10.1016/j.clsr.2020.105430.

Veale, Michael, and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act." Computer Law Review International 22, no. 4 (2021): 97–112. https://doi.org/10.9785/cri-2021-220402.

Wacks, Raymond. Privacy and Media Freedom. Oxford: Oxford University Press, 2013.

World Bank. Digital Identity for Inclusive and Trusted Public Services. Washington, DC: World Bank, 2024.

Yeung, Karen, and Martin Lodge. "Algorithmic Regulation and Accountability." Regulation & Governance 16, no. 3 (2022): 629–44. https://doi.org/10.1111/rego.12406

Yeung, Karen. "Algorithmic Regulation: A Critical Interrogation." Regulation & Governance 12, no. 4 (2018): 505–23.

Zarsky, Tal Z. "Transparent Predictions." University of Illinois Law Review (2013): 1503–70.