JAMBURA LAW REVIEW

Volume 7 Issue 02
JALREV 7 (2) 2025

July 2025
ISSN Print: 2654-9266
ISSN Online: 2656-0461

Legal Challenges of the Application of the Right to Be Forgotten in Blockchain in Indonesia and the European Union

Uni Tsulasi Putri[1]✉
Irna Nurhayati[2]
Taufiq El Rahman[3]

[1]Universitas Gadjah Mada; Universitas Ahmad Dahlan, Indonesia
[2,3]Universitas Gadjah Mada, Indonesia.

✉ uni.tsulasi.p@mail.ugm.ac.id

Article Info

Submitted: Feb 5, 2025
Revised: Jul 9, 2025
Accepted: Jul 31, 2025

Keywords:
Blockchain; Right to Be Forgotten; Data Protection Law; EU GDPR; Immutability.

How to cite *[Chicago Manual of Style 17th edition (full note)]:*
Uni Tsulasi Putri, Irna Nurhayati, Taufiq El Rahman, "Legal Challenges of the Application of the Right to Be Forgotten in Blockchain in Indonesia and the European Union" *Jambura Law Review* 7, no. 2 (2025): 633–663.

Abstract

The Right to Be Forgotten (RTBF), as enshrined in data protection laws under Article 8 of the Indonesia's Personal Data Protection Law (PDP Law) and Article 17 of the European Union (EU) General Data Protection Regulation (GDPR), grants individuals the right to request the deletion of personal data. However, this principle is fundamentally at odds with blockchain's immutability, which ensures that once recorded, data cannot be altered or erased. This study examines the legal conflict between RTBF and blockchain through a doctrinal and comparative legal analysis of Indonesia and the EU regulatory framework. This study employs a normative legal research approach, utilizing doctrinal analysis and comparative legal method to examine statutory provisions, case law, and scholarly literature of Indonesia and the EU on the conflict between the RTBF and blockchain technology. Findings reveal that both jurisdictions struggle to reconcile RTBF enforcement with blockchain's technical architecture, particularly in public networks. While the EU possesses stronger institutional maturity, it lacks clear jurisprudential direction on blockchain-based RTBF cases. Indonesia, with its evolving legal landscape, shows potential for flexible reinterpretation of "data destruction" under Article 44 of the PDP Law. The paper proposes a normative shift interpretation from the right to absolute erasure of the data itself toward the right to cryptographic erasure which supported by hybrid legal-technical solutions such as key deletion, off-chain storage, and permissioned blockchains.

1. Introduction

These advancements in information and communication technology have profoundly impacted human civilisation worldwide.[1] Search engines, and websites have made it easy to find almost any topic online.[2] The increasing digitization of personal data has transformed the landscape of privacy rights in the modern era. The increasing reliance on digital technologies and online databases brought renewed attention to privacy concerns, emphasizing the need for a legal framework that allows individuals to control their digital footprints.[3] As digital footprints become virtually permanent, the Right to Be Forgotten (RTBF) has emerged as one of the legal mechanisms to empower individuals in protecting their personal information from unjustified public exposure.

The RTBF grants individuals the ability to request the removal, delisting, or modification of personal data available online if it is inaccurate, outdated, irrelevant, or potentially damaging to their reputation.[4] Its concept originated from continental penal law, where individuals could request the erasure of records related to past offenses after demonstrating social rehabilitation.[5] This right gained significant legal recognition through the Google Spain case, where the Court of Justice of the European Union (CJEU) ruled that individuals within the European Union (EU) have the authority to demand the erasure of certain personal information from search engine results, establishing RTBF as a fundamental aspect of EU law.[6]

---

[1] Sheila Kusuma Wardani Amnesti et al., "Legal Protection of Personal Data Security in Indonesian Local Government Apps: Al Farabi's Perspective," *Legality : Jurnal Ilmiah Hukum* 33, no. 1 (2024): 1–19, https://doi.org/10.22219/ljih.v33i1.34623.

[2] Jehad D. Aljazi, "The Right of Local Government Employees to Expungement of Disciplinary Offences Processed Digitally in Jordanian and Qatari Legislation," Legality : Jurnal Ilmiah Hukum 33, no. 1 (2024): 20–43, https://doi.org/10.22219/ljih.v33i1.36212.

[3] N N G de Andrade, "Oblivion: The Right to Be Different … from Oneself: Re-Proposing the Right to Be Forgotten," in Palgrave Macmillan Memory Studies (2014), https://doi.org/10.1057/9781137428455_5.

[4] M J Kelly and D Satola, "The Right to Be Forgotten," University of Illinois Law Review 2017, no. 1 (2017): 1–64.

[5] J Stoddart, "Lost in Translation: Transposing the Right to Be Forgotten from Different Legal Systems," in The Right to Be Forgotten: A Canadian and Comparative Perspective (2020), https://doi.org/10.4324/9781003017011-2.

[6] T D Oganesian, "Legal Framework, Limits and Standards for the Application of the Right to Be Forgotten: The Experience of the European Union," Vestnik Sankt-Peterburgskogo Universiteta. Pravo 14, no. 3 (2023): 750–67, https://doi.org/10.21638/spbu14.2023.312.

Article 17 of the EU GDPR, which has been in effect since May 25, 2018, grants individuals the right to request the deletion of their personal data without undue delay if certain conditions are met.[7] In Indonesia, Under Article 8 of the 2022 Personal Data Protection Act, data subjects also have the right to terminate the processing of their personal data, request its deletion, and/or demand its destruction in accordance with the applicable laws and regulations. Previously, under Article 26 of the Indonesia's Electronic Information and Transactions (EIT) Law which has been amended by Law No. 19 of 2016, provided the rights of individuals to request deletion of irrelevant Electronic Information and/or Electronic Document. The obligation is bound towards every Electronic System Operator. Under the 2016 EIT Law, the request to data deletion/erasure requires judicial approval.

However, the presence of RTBF is now being questioned by the rapid emergence of blockchain technology that introduces new standards of data integrity and trust.[8] Its two defining features, immutability and decentralization, distinguish blockchain from traditional databases and present unique legal challenges. Immutability ensures that once data is recorded on the blockchain,[9] it becomes nearly impossible to alter or delete due to cryptographic mechanism and consensus protocols.[10] Furthermore, decentralization eliminates reliance on a central authority by distributing control across a network of nodes, making it difficult to identify a singular data controller responsible for processing personal data.[11]

---

[7] https://gdpr-info.eu/art-17-gdpr/

[8] D K Kumar et al., "Comparative Analysis of Transaction Speed and Throughput in Blockchain and Hashgraph: A Performance Study for Distributed Ledger Technologies," Journal of Machine and Computing 3, no. 4 (2023): 497–504, https://doi.org/10.53759/7669/jmc202303041; R Moondra et al., "EthFor: Forensic Investigation Framework for Ethereum Blockchain," Lecture Notes in Networks and Systems 765 LNNS (2023): 481–88, https://doi.org/10.1007/978-981-99-5652-4_43.

[9] Chen Siqi et al., "Application of Blockchain Technology in Cross-Border Telecommunications Network Fraud to Ensure China's Judicial Justice," *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 3 (2024): 472–86, https://doi.org/10.29303/ius.v12i3.1554.

[10] J Shah and S Parveen, "Understanding the Blockchain Technology Beyond Bitcoin," Lecture Notes in Mechanical Engineering, 2021, 499–516, https://doi.org/10.1007/978-981-33-4320-7_45.

[11] M Devisri et al., "Blockchain Innovations for Secure Online Transactions," in Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning (2024), https://doi.org/10.4018/979-8-3693-6557-1.ch021; M Imam and K Saini, "A Review of Applications and Security: Blockchain Technology," in Blockchain and EHR (2024); S Aghili, Leveraging Blockchain Technology: Governance, Risk, Compliance, Security, and Benevolent Use Cases, in Leveraging Blockchain Technology: Governance, Risk, Compliance, Security, and Benevolent Use Cases (2024), https://doi.org/10.1201/9781003462033.

While these features enhance security[12] and transparency,[13] they directly conflict with the legal requirements under the RTBF, which mandates data controllers to delete or modify personal data upon request.

Several academic discourse on RTBF and blockchain primarily concentrates on technical solutions. Parikh, Sural, Atluri, and Vaidya address the privacy concerns arising from users' limited visibility and control over their personal information, which are amplified by complex compliance requirements under the GDPR and California Consumer Privacy Act (CCPA).[14] In response to the RTBF provisions under GDPR, they propose CRISP (Consensus-enabled, Redactable, Immutable, Securely shareable, Provable), a permissioned enterprise blockchain framework enabling trustless interoperation among a network of identifiable organizations to support RTBF.[15] CRISP integrates off-chain data storage, distributed resource sharing, blockchain consensus mechanisms, and decentralized access control.[16]

Ikemefuna-Amaechi also highlights that the immutable nature of blockchain presents a significant obstacle to implementing the GDPR's RTBF, as the technology inherently resists modification or deletion of data once recorded.[17] To address this conflict, the Ikemefuna-Amaechi discusses several potential solutions, including the use of off-chain storage mechanisms, where personal data is stored outside the blockchain and only references or hashes are recorded on-chain.[18] This would allow the actual data to be modified or deleted off-chain, aligning better with GDPR requirements while

[12] Moondra et al., "EthFor: Forensic Investigation Framework for Ethereum Blockchain"; P Thilakavathy et al., "Investigating Blockchain Security Mechanisms for Tamper-Proof Data Storage," 2023 International Conference on Communication, Security and Artificial Intelligence, ICCSAI 2023, 2023, 926–30, https://doi.org/10.1109/ICCSAI59793.2023.10421006.
[13] Aghili, Leveraging Blockchain Technology: Governance, Risk, Compliance, Security, and Benevolent Use Cases.
[14] Anand Manojkumar Parikh et al., "Enabling Right to Be Forgotten in a Collaborative Environment Using Permissioned Blockchains," in Data and Applications Security and Privacy XXXIX, ed. Sokratis Katsikas and Basit Shafiq (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-031-96590-6_9.
[15] Ibid.
[16] Ibid.
[17] Stacy Ogechukwu Ikemefuna-Amaechi, "Balancing Privacy and Innovation: Exploring the Conflict Between Data Protection Rights and Blockchain's Immutability and Decentralized Nature," in Master's Thesis in EU Law, with a Specialization in Data Protection Law (Uppsala Universitet, 2025).
[18] Ibid.

maintaining blockchain's integrity. Additionally, techniques such as data anonymization and encryption are considered to further mitigate risks, while regulatory strategies may involve designing blockchain systems that incorporate built-in mechanisms for data amendment or erasure without compromising security or transparency.[19]

Anand Manojkumar Parikh et al and Ikemefuna-Amaechi focus on legal-technical or even technical-based solutions such as off-chain storage, encryption, anonymization, and redactable blockchains to resolve the RTBF–blockchain conflict. While useful, these studies centre on technology and do not address the legal interpretation of RTBF or its application in different jurisdictions. On the other hand, Modestos Gavalas examines conflicts including the identification of data controllers and the applicability of GDPR to decentralized systems.[20] He proposes solutions not only focusing on pseudonymization, but also flexible interpretations of deletion, and the involvement of centralized authorities in permissioned networks.[21] Gavalas concludes that a case-by-case approach is necessary to achieve GDPR compliance while maintaining blockchain's core functionality, emphasizing cooperation between legal and technical fields.[22]

Those existing studies provide valuable insights into technical strategies for reconciling RTBF with blockchain's immutable architecture. However, most of them concentrate on technical mechanisms and lack an in-depth exploration of the philosophical basis and legal interpretation of RTBF, particularly in a comparative jurisdictional context. Moreover, most existing research concentrates on the EU's GDPR, while discussions of Indonesia's emerging PDP framework remain limited. This creates a gap for research that examines not only the technological aspects but also how different legal systems, such as Indonesia and the EU, interpret and apply RTBF in blockchain environments. Therefore, a comparative approach to examine the

[19] Ibid.
[20] Modestos Gavalas, "Does Blockchain Technology Per Se Constitute a Breach of the GDPR? An Effort to Harmonize Two Seemingly Opposing Concepts," Global Privacy Law Review (Alphen aan den Rijn, The Netherlands), Kluwer Law International, 2025, 66–72.
[21] Ibid.
[22] Ibid.

philosophical and regulatory framework of RTBF and personal data protection in Indonesia and the EU is necessary in this study.

The normative justification of the comparison is because the EU's GDPR serves as the global benchmark for data protection, including the RTBF, and Indonesia's PDP Law was explicitly designed with the intention of aligning its standards with those of advanced jurisdictions. As stated in the Academic Paper for the Bills of the PDP Law, one of the legislative backgrounds of PDP Law's urgency is to ensure that Indonesia provides a level of personal data protection equivalent to other countries.[23] This alignment aims to place Indonesia on the same level as countries with advanced data protection laws.[24] It also helps strengthen Indonesia's reputation as a trusted business hub, which supports the country's national economic growth strategy.[25]

This paper addresses these issues through a doctrinal and comparative legal analysis of Indonesia and the EU. Analyzing both jurisdictions provides a doctrinal foundation to evaluate how a mature legal system of the EU, operationalizes RTBF, offering a reference point for potential refinement of Indonesia's normative approach. This study will identify normative alignments, regulatory gaps, and practical lessons that can guide Indonesia in refining its RTBF application in blockchain contexts.

2. Problem Statement

The conflict between RTBF and blockchain technology raises fundamental legal challenges, particularly regarding the enforceability of data erasure rights in decentralized systems. While the RTBF is intended to empower individuals to control their personal data, blockchain's immutable and decentralized nature makes data erasure technically complex and legally contentious. Despite the RTBF's recognition in the EU GDPR and Indonesia's PDP Law, significant gaps remain in understanding how this right can be effectively implemented within blockchain environments. Therefore, this study seeks to explore these challenges by addressing three key questions: first, how RTBF is regulated and applied in Indonesia and the EU; second, what legal conflict

[23] Kemenkumham, "Naskah Akademik RUU Perlindungan Data Pribadi," Kementerian Hukum Dan Hak Asasi Manusia, 2022, 121.
[24] Ibid.
[25] Ibid.

arise from the interaction between RTBF and blockchain's nature; and third, what legal or regulatory approaches can accommodate the application of RTBF to blockchain system.

3. Methods

This study adopts normative legal research approach, focusing on analysis of laws, regulations and scholarly writings to examine the conceptual coherence of the RTBF in blockchain environments. Legal knowledge in this context is derived from authoritative texts, including statutes, case law, and writings of legal scholar. This method is employed to critically interrogate the legal gap between the regulation concerning the RTBF and the technical immutability and decentralized nature of blockchain systems, as outlined in the problem statement.

A comparative approach is employed to assess how two distinct legal systems–the EU and Indonesia–address the same legal issue which is enforcing RTBF within decentralized, immutable blockchain systems. The EU represents a mature data protection regime under 2016 EU GDPR with established jurisprudence, while Indonesia provides a perspective as an emerging regulatory system under 2022 PDP Law. This comparison highlights how regulatory maturity affect the application of RTBF in decentralized contexts. Data collection relied on library research of primary legal materials (laws, case law) and secondary legal materials (scholarly articles and other academic publications).

4. The Philosophical Ground and Legal Foundations of the Right to be Forgotten (RTBF) in Indonesia and the EU

The state has a responsibility to guarantee order and security, including in terms of personal data.[26] The philosophical basis for the protection of the RTBF in Indonesia is grounded in Pancasila and the 1945 Constitution. Indonesia, as a State of rule of law based on Pancasila, obliged to protect human dignity and rights which crystalized under the Pancasila principles. Pancasila was designed to reflect substantive values

[26] Arief Budiman et al., "Wājibah Will for Non-Muslim Heirs in Indonesia: A Legal Political Perspective Based on Justice and Welfare," Ijtihad : Jurnal Wacana Hukum Islam Dan Kemanusiaan 24, no. 2 (2024): 223–50, https://doi.org/10.18326/ijtihad.v24i2.223-250.

aligned such social justice.[27] The second principle of Pancasila, known as "Just and Civilized Humanity", serves as the philosophical foundation for personal data protection, and therefore, become the philosophical basis of RTBF.[28] This is based on the understanding that such protection fosters justice and contributes to the development of a human civilization that respects and values personal data.

In this framework, the vast majority of data and information is now digital.[29] The RTBF functions as a legal manifestation of constitutional guarantees, ensuring that individuals retain control over their personal information in the digital era.[30] It reflects the balance central to Indonesian legal philosophy that is safeguarding individual autonomy and dignity while accommodating lawful data processing for the public interest and technological innovation. The integration of Pancasila values into the PDP Law positions the RTBF as a means to harmonize justice and society's welfare in the middle of technological advancement.[31]

Initially, Indonesia's Electronic Information and Transactions Law (EIT Law) No. 11 of 2008 did not include RTBF provisions. However, the law was then amended under Law No. 19 of 2016, incorporating RTBF into Article 26. This amendment provided individuals with the legal means to request the removal of personal data from digital platforms, particularly when it is misleading, irrelevant, or harmful. Under the 2016 ITE Law, the request to data erasure requires judicial approval.[32] This means that an

[27] Ahmad Yani Anshori and Landy Trisna Abdurrahman, "Constitutional Contestation of the Islamic State Concept in the Indonesian Parliament 1956-1959," De Jure: Jurnal Hukum Dan Syar'iah 16, no. 2 (2024): 278–316, https://doi.org/10.18860/j-fsh.v16i2.29572.
[28] Kemenkumham, "Naskah Akademik RUU Perlindungan Data Pribadi."
[29] Omar Farouk Al Mashhour et al., "Estate Planning in the Digital Age: Rufadaa as a Lesson to Be Learnt to Improve the Syrian Personal Status Law," Brawijaya Law Journal 11, no. 1 (2024): 72–90, https://doi.org/10.21776/ub.blj.2024.011.01.04.
[30] Kukuh Tejomurti et al., "Big Data Analytics Algorithms for Dynamic Pricing: The Legal Analysis of the Indonesia Competitions Law Readiness in Digital Era," *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 1 (2024): 68–90, https://doi.org/10.29303/ius.v12i1.1303.
[31] Kemenkumham, "Naskah Akademik RUU Perlindungan Data Pribadi."
[32] Sriono et al., "Legal Protection for Digital Bank Customers in Indonesia: Analysis of Data Confidentiality Regulations and Bank Responsibility," *LITIGASI* 25, no. 2 (2024): 301–30, https://doi.org/10.23969/litigasi.v25i2.18538; Dwi Suryahartati et al., "Tradisi Hukum Dan Inovasi Digital: Menakar Posisi Produk E- Notary Pada Sengketa Perdata: Legal Tradition and Digital Innovation: Assessing the Position of e-Notary Products in Civil Disputes," *LITIGASI* 26, no. 1 (2025): 409–47, https://doi.org/10.23969/litigasi.v26i1.19193; Lutfi Chakim et al., "Fatwa, Authority, and Digital Trade: A Critical Legal-Discursive Analysis of Dropshipping Rulings in Indonesia and Egypt," *Jurisdictie: Jurnal Hukum Dan Syariah* 16, no. 1 (2025): 124–65, https://doi.org/10.18860/j.v16i1.31882; Ria Setyawati et al., "Data Driven Dominance in Digital Markets: Assessing Indonesian Competition Law in the Digital

individual must first obtain a court order before any online platform is legally obligated to remove the content. Even though there is a second amendment of the 2008 Indonesian EIT Law based on the Law No. 1 of 2024, there was no specific amendment regarding the regulation under Article 26 of the 2016 Indonesian EIT Law.

The development of the RTBF in Indonesia is also regulated in the Personal Data Protection Law No. 27 Year 2022 (PDP Law) which is established and took effect on 17 October 2022. Article 8 of the PDP Law grants individuals (data subjects) the right to control their personal data by requesting the cessation of processing, deletion, or destruction of their data. However, these rights must be exercised in compliance with existing legal provisions, ensuring that data removal aligns with regulatory frameworks. Article 4 divide personal data into two categories: specific personal data and general personal data. The former consist of (a) health data and information; (b) biometric data; (c) genetic data; (d) criminal records; (e) children's data; (f) personal confidential data; and/or; (g) other data as regulated by applicable laws and regulation. The latter consist of (a) full name; (b) gender; (c) nationality; (d) religion; (e) marital status; and/or; (f) personal data that, when combined, can be used to identify an individual.

Under Article 44, Section (1), Letter (b) of the PDP Law, personal data controllers are required to "destroy" personal data upon request from the data subject. Personal Data Controllers is defined in article 1 number 4 as an entity or individual responsible for "determining the objectives and overseeing the processing of personal data." It establishes that control can be exercised individually or collaboratively, ensuring accountability in data governance. Furthermore, the term "destroy" in that article is defined in the explanation as "the act of eliminating, erasing, or destructing personal data to the extent that it can no longer be used to identify the data subject."

Article 2 of the Indonesian PDP Law establishes the scope of applicability of the law. Under article 1 number 1, personal data refers to any information related to an identifiable individual, whether the identification is direct or indirect, independently

Age," *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 2 (2024): 264–84, https://doi.org/10.29303/ius.v12i2.1377.

or in combination with other information, through electronic or non-electronic systems. This broad definition ensures that any data capable of identifying a person falls under the protection of the law. To safeguard personal data, personal data protection encompasses a comprehensive set of measures applied throughout the data processing cycle. These measures are designed to uphold the constitutional rights of data subjects, ensuring their privacy and data security (Article 1 number 2 PDP Law). The law recognizes that the protection of personal data is a fundamental right, reinforcing accountability among data controllers and processors.

It applies not only to individuals, public entities, and international organizations operating within Indonesia but also to those outside Indonesia if their activities have legal consequences within the country or affect Indonesian citizens' personal data, regardless of their location. This provision ensures that data protection obligations extend beyond national borders, particularly when Indonesian data subjects are involved (Article 2 PDP Law).

Given the broad definition of personal data under the PDP Law, blockchain technology can potentially fall within its scope when it involves identifiable personal data. While blockchain is designed to be decentralized and immutable, personal data recorded on a blockchain, whether directly or indirectly, may still be subject to data protection obligations. The challenge, however, lies in the inherent immutability of blockchain, which conflicts with certain legal requirements, such as the Right to be Forgotten as also regulated in the PDP Law.

The RTBF in the EU has undergone significant evolution, driven by the growing challenges of digitalization, online permanence, and the need to balance privacy rights with freedom of expression.[33] The philosophical basis of the RTBF in the EU GDPR is anchored in the principles of privacy and data protection as provided in Articles 7 and

[33] B Sobkow, "Forget Me, Forget Me Not - Redefining the Boundaries of the Right to Be Forgotten to Address Current Problems and Areas of Criticism," Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 10518 LNCS (2017): 34–51, https://doi.org/10.1007/978-3-319-67280-9_3; Kelly and Satola, "The Right to Be Forgotten."

8 of the Charter of Fundamental Rights (CFR) of the EU.[34] Article 8 of the CFR of the EU recognizes the protection of personal data as a distinct and autonomous fundamental right, separate from the right to privacy under Article 7. It affirms that everyone is entitled to the protection of their personal data, which must be processed fairly, for specified purposes, and on the basis of consent or another legitimate legal ground. This principle ensures that personal data cannot be processed arbitrarily and that individuals retain meaningful control over its use. The provision further grants individuals the right to access their personal data and to request rectification.

The RTBF, as introduced in the EU DGPR underlies its philosophical basis on the balancing process which revolves around the tension between fundamental rights such as privacy and data protection, and the rights to free expression and access to information. This tension necessitates a balancing act grounded in normative principles that aim to protect individual autonomy while safeguarding societal interests.[35] This balance ensures that the RTBF does not lead to unjustified censorship, maintaining harmony between the protection of individual dignity and the preservation of democratic transparency.[36]

In 2012, the European Commission proposed the RTBF as part of a broader data protection reform initiative. This proposal aimed to strengthen individuals' control over their personal data and ensure greater accountability among data controllers.[37] A landmark moment in the development of the RTBF occurred in 2014, when the Court of Justice of the European Union (CJEU) issued a ruling in the Mario Costeja González

[34] M Von Grafenstein and W Schulz, "The Right to Be Forgotten in Data Protection Law: A Search for the Concept of Protection," International Journal of Public Law and Policy 5, no. 3 (2015): 249–69, https://doi.org/10.1504/IJPLAP.2015.075049; M R Leiser, "'Private Jurisprudence' and the Right to Be Forgotten Balancing Test," Computer Law and Security Review 39 (2020), https://doi.org/10.1016/j.clsr.2020.105458.
[35] Leiser, "'Private Jurisprudence' and the Right to Be Forgotten Balancing Test."
[36] Von Grafenstein and Schulz, "The Right to Be Forgotten in Data Protection Law: A Search for the Concept of Protection"; Leiser, "'Private Jurisprudence' and the Right to Be Forgotten Balancing Test"; Oganesian, "Legal Framework, Limits and Standards for the Application of the Right to Be Forgotten: The Experience of the European Union"; G Sartor, "The Right to Be Forgotten: Balancing Interests in the Flux of Time," International Journal of Law and Information Technology 24, no. 1 (2016): 72–98, https://doi.org/10.1093/ijlit/eav017.
[37] A De Baets, "A Historian's View on the Right to Be Forgotten," International Review of Law, Computers and Technology 30, nos. 1–2 (2016): 57–66, https://doi.org/10.1080/13600869.2015.1125155.

v. Google Spain case.[38] The case arose when Mario Costeja González requested the removal of outdated financial information from Google's search results, arguing it was no longer relevant. The CJEU ruled that search engines are responsible for processing personal data and must remove links to personal information if it is inaccurate, irrelevant, or excessive, unless there is a public interest in retaining it.[39]

The court held that individuals could request search engines to delist personal information if it was inadequate, irrelevant, or excessive. This decision established the RTBF as a fundamental legal right within the EU and set a precedent for similar regulations worldwide.[40] The RTBF was later codified into law through the General Data Protection Regulation (GDPR), which came into effect in May 25th, 2018.

The GDPR provides detailed guidelines on when and how personal data can be erased, reinforcing the right of individuals to request data removal while balancing it with other legal and public interest considerations.[41] The RTBF established under Article 17 of the GDPR, grants individuals the ability to request the erasure of their personal data under specific circumstances, such as when the data is no longer necessary, consent has been withdrawn (Article 6(1)(a)), or the data has been unlawfully processed. However, this right is not absolute and must be weighed against legal obligations (Article 6(1)(c)), public interest considerations (Article 6(1)(e)), and legitimate interests (Article 6(1)(f)).

A limitation to the RTBF is the lawfulness of processing outlined in Article 6. This article ensures that data processing is only lawful if it meets one of the listed conditions, such as fulfilling contractual obligations, complying with legal requirements, or serving the public interest. Additionally, Article 8 imposes stricter conditions for obtaining a child's

[38]Heribertus Untung Setyardi, "Right To Be Forgotten Vis-À-Vis Hak Atas Informasi," Jurnal Kewarganegaraan 8, no. 1 (2024): 1096–108, https://doi.org/10.31316/jk.v8i1.6529.
[39] ase C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja. González (May 13, 2014).
[40] M L Jones et al., "The Right to Be Forgotten," Proceedings of the Association for Information Science and Technology 52, no. 1 (2015): 1–3, https://doi.org/10.1002/pra2.2015.145052010010; Sobkow, "Forget Me, Forget Me Not - Redefining the Boundaries of the Right to Be Forgotten to Address Current Problems and Areas of Criticism."
[41] A N Vavra, "The Right to Be Forgotten: An Archival Perspective," American Archivist 81, no. 1 (2018): 100–111, https://doi.org/10.17723/0360-9081-81.1.100; Oganesian, "Legal Framework, Limits and Standards for the Application of the Right to Be Forgotten: The Experience of the European Union."

consent for data processing in digital services,[42] which is particularly relevant to cases where the RTBF applies to minors' personal data collected online. Furthermore, Article 9 strengthens data protection by prohibiting the processing of special categories of personal data, including biometric and health data, unless specific exceptions apply, such as explicit consent or public health purposes. If such sensitive data is processed without meeting these conditions, data subjects could invoke the RTBF to request its removal.

Finally, Article 21 complements the RTBF by granting individuals the right to object to the processing of their personal data, particularly when based on legitimate interests (Article 6(1)(f)) or public interest tasks (Article 6(1)(e)). This article is particularly relevant to cases where individuals challenge data retention policies or oppose direct marketing and profiling, reinforcing their ability to control how their data is used.

Under Article 4 GDPR, personal data is defined as any information relating to an identified or identifiable natural person ("data subject"). This includes names, identification numbers, location data, online identifiers, and factors related to a person's physical, physiological, genetic, mental, economic, cultural, or social identity. The regulation applies not only to standard personal data but also to special categories of personal data (e.g., health data, racial or ethnic origin, biometric data), which are afforded additional protections.

The GDPR establishes clear roles and responsibilities for data actors. It protects natural persons (data subjects) and regulates entities that process their data, specifically: (1) Data Controllers or Entities that determine the purposes and means of processing personal data; (2) Data Processors, which means Organizations or individuals that process personal data on behalf of a controller; (3) Supervisory Authorities, which defined as Independent public authorities that oversee the enforcement of GDPR in each Member State.

One of the key aspects of the GDPR is its broad scope of applicability. The GDPR applies extraterritorially, meaning that any organization, regardless of its geographic location,

[42] Tejomurti et al., "Big Data Analytics Algorithms for Dynamic Pricing."

must comply with GDPR provisions if it processes the personal data of individuals within the EU. This ensures that companies operating outside the EU but handling EU residents' data are still subject to its regulations.

Before the EU formally introduced the RTBF, some European countries like Germany, France and Italy had already implemented similar legal frameworks to provide individuals with greater control over their data.[43] Germany, for example, included provisions in its Federal Data Protection Act (*Bundesdatenschutzgesetz*) of 1977, which allowed individuals to request the deletion of stored personal data if its retention was deemed unlawful or no longer necessary.[44]

While Indonesian PDP Law adopts similar privacy principles as GDPR, including the right to erasure, the legal infrastructure to operationalize RTBF remains underdeveloped. Indonesian data subjects must often seek judicial authorization before data removal, and supervisory authorities have yet to issue detailed implementation guidelines. The PDP Law also distinguishes between general and specific personal data, establishing differentiated protection levels, but lacks a nuanced interpretation of how RTBF should be enforced in complex technological environments.

A crucial doctrinal point in both jurisdictions is the conditional nature of RTBF. It is not an automatic right to delete data in all situations. Instead, it depends on the context and must be balanced against other important rights, like freedom of expression or public interest. Koops emphasizes the complexities and limitations associated with implementing RTBF, such as practical challenges in data deletion, retention periods, and balancing individual rights with legal obligations and public interests.[45] For instance, he notes the difficulty of exercising a right to delete data when there are legal retention obligations, implying a need to balance this right against other legal

[43] M Mach, "The Right to Be Forgotten in Response to the Development of Information Technology," Pravnik 160, no. 7 (2021): 597–609.
[44] Ibid. P. 600.
[45] Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows. A Critical Analysis of the 'Right To Be Forgotten' in Big Data Practice," SCRIPTed 8, no. 3 (2011): 1–28, https://doi.org/10.2966/scrip. P, 20, 26 – 28.

requirements.[46] Furthermore, the challenge of determining when data are no longer relevant highlights a nuanced approach rather than an automatic override of other rights.

In addition, the discussions about the limitations of a strong deletion right, especially in the context of legal obligations and legitimate processing, suggest an emphasis on balancing interests rather than automatic prioritization. The mention of challenges such as data retention laws, statutory obligations, and the potential for harm during legitimate processing periods reflects an awareness of the need for proportionality and careful balancing in applying RTBF.[47] This perspective is reflected in GDPR's multiple balancing tests and, to a lesser extent, in Indonesia's broad exemptions tied to legal compliance and public interest objectives.

The GDPR explicitly codifies this balancing mechanism in Article 17(3), which lists several exceptions to the right to erasure, including public interest in health, legal obligations, and the exercise of freedom of expression. Although Indonesia's PDP Law lacks similarly detailed provisions, it nevertheless includes general exemptions for legal compliance and public interest considerations, reflecting an incipient recognition of the qualified nature of RTBF in Indonesian law.

When compared to the EU's GDPR, the Indonesian PDP Law adopts similar normative principles but lacks detailed provisions or technical guidance on how the RTBF should operate in blockchain environments. The EU addresses this gap through interpretive guidance from supervisory authorities, such as CNIL, without amending the core GDPR.[48][49]In Indonesia, the absence of comparable guidance creates legal uncertainty for blockchain operators and data subjects. A revision of Indonesia's regulatory

[46] Ibid. P. 20.
[47] Ibid. P. 20, 26 – 28.
[48] A Jambert, "Blockchain and the GDPR: A Data Protection Authority Point of View," Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 11469 LNCS (2019): 3–6, https://doi.org/10.1007/978-3-030-20074-9_1.
[49] Ibid.; Z Chousein et al., "Tension between GDPR and Public Blockchains: A Data-Driven Analysis of Online Discussions," ACM International Conference Proceeding Series, 2020, https://doi.org/10.1145/3433174.3433587; M K S Suripeddi and P Purandare, "Blockchain and GDPR - A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing," Journal of Physics: Conference Series 1964, no. 4 (2021), https://doi.org/10.1088/1742-6596/1964/4/042005.

framework is therefore necessary—not in the form of amending the PDP Law itself, but through the issuance of implementing regulations or technical guidelines by the related Authority.

In summary, both the European Union and Indonesia recognize RTBF, but their legal frameworks assume centralized control and enforceability. Blockchain's decentralized and immutable nature creates tensions with RTBF, challenging its practical application and raising questions about how privacy rights can adapt to evolving technology.

5. The Paradox Between the Right to Be Forgotten (RTBF) and Blockchain's Immutability Nature

5.1. Immutable Nature of Blockchain

The philosophical basis of blockchain's immutability lies in its foundational principles of decentralization, transparency, and trust. These principles work together to ensure that once data is recorded on the blockchain, it cannot be altered or deleted, thereby establishing a reliable and tamper-proof ledger. Decentralization ensures that no single entity has unilateral control over the entire network, which prevents any single participant from altering data without collective agreement.[50] Transparency strengthens this integrity by making all transactions visible to participants, ensuring that any attempted modification would be immediately detected.[51] Trust emerges as a natural consequence of immutability, participants can rely on the accuracy and integrity of recorded information, assured that it has not been manipulated.[52] From a

[50] G Wang and M Nixon, "SoK: X-Assisted BFT Consensus Protocols," Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 14206 LNCS (2023): 54–71, https://doi.org/10.1007/978-3-031-44920-8_4; G Wang and M Nixon, "SoK: Essentials of BFT Consensus for Blockchains," 2023 5th International Conference on Blockchain Computing and Applications, BCCA 2023, 2023, 315–28, https://doi.org/10.1109/BCCA58897.2023.10338868; A Abdul-Wadud et al., "Blockchain Technology: Evolution, Potentials, and Operational Challenges," in The Intersection of Blockchain and Energy Trading: Exploring Decentralized Solutions for Next-Generation Energy Markets (2024), https://doi.org/10.1016/B978-0-443-23627-3.00003-X.

[51] Abdul-Wadud et al., "Blockchain Technology: Evolution, Potentials, and Operational Challenges"; F Anwar et al., "Comprehensive Insight into Blockchain Technology: Past Development, Present Impact and Future Considerations," International Journal of Advanced Computer Science and Applications 13, no. 11 (2022): 878–907, https://doi.org/10.14569/IJACSA.2022.01311101.

[52] H Wang et al., "A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges," IEEE Internet of Things Journal 10, no. 16 (2023): 14671–88, https://doi.org/10.1109/JIOT.2023.3278329; Q Liu and J Shen, "K-Time Redactable Blockchain with Decentralized History Rewriting," Proceedings - 2023 International Conference on Data Security and Privacy Protection, DSPP 2023, 2023, 41–49, https://doi.org/10.1109/DSPP58763.2023.10404463.

technical perspective, immutability is supported by consensus protocols and cryptographic hash functions. Consensus mechanisms, such as Proof-of-Work (PoW) and Byzantine Fault Tolerance (BFT), require network-wide agreement on the blockchain's state, making it nearly impossible for a single node to alter records without majority validation.[53] Similarly, cryptographic hash functions link each block to its predecessor in a chain, such that any modification to a block changes its hash and disrupts the chain's integrity, exposing tampering.[54]

Despite its strengths, blockchain's immutability presents challenges when intersecting with regulatory requirements like the GDPR's RTBF, which demands the capacity to delete or modify personal data. Furthermore, immutability can become a liability when malicious or illegal content is recorded on-chain, as it cannot be easily removed. Moreover, blockchain is not uniform. Public blockchains like Bitcoin is fully decentralized, making it impossible to identify data controllers and enforce RTBF. Private or permissioned blockchains, on the other hand, often used in enterprises, are managed by identifiable entities, allowing more controlled governance and RTBF compliance.

5.2. The Conceptual and Regulatory Tensions Between the RTBF and Blockchain Technology

The implementation of the RTBF within blockchain technology, especially public blockchain, presents significant challenges due to the inherent nature of blockchain systems. While blockchain's immutability and decentralization provide security and trust, they also create conflicts with legal requirements that mandate data deletion or modification upon user request.

---

[53] Wang and Nixon, "SoK: Essentials of BFT Consensus for Blockchains"; Wang and Nixon, "SoK: X-Assisted BFT Consensus Protocols"; S Sharma et al., "Consensus Mechanisms Analysis: A Remedy for the Byzantine Generals Problem," Proceedings - International Conference on Technological Advancements in Computational Sciences, ICTACS 2023, 2023, 674–78, https://doi.org/10.1109/ICTACS59847.2023.10390006.

[54] Sharma et al., "Consensus Mechanisms Analysis: A Remedy for the Byzantine Generals Problem"; P Mukherjee and C Pradhan, "Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology," in Intelligent Systems Reference Library, vol. 203 (2021), https://doi.org/10.1007/978-3-030-69395-4_3.

The fundamental principle of the RTBF is that individuals have the right to request the deletion of their personal data when it is no longer necessary, inaccurate, or unlawfully processed. This principle, enshrined in Article 17 of the GDPR and Article 8 of Indonesia's PDP Law, reflects the growing need for individuals to regain control over their digital footprint. However, this right clashes with blockchain's immutability, which ensures that data cannot be altered or deleted once recorded, enhancing security and integrity. While immutability prevents unauthorized modifications, it also makes compliance with privacy laws like GDPR challenging, as blockchain lacks a mechanism for data erasure on request.[55]

The EU GDPR and Indonesia's PDP Law both establish mechanisms for data subjects to exercise their right to request data deletion. Article 44 of the PDP Law even mandates that data controllers must destroy personal data upon request from the data subject. However, in blockchain networks, there is no single entity or "data controller" with the authority to enforce deletion, making it nearly impossible to comply with such regulations. This raises legal and ethical concerns about whether blockchain-based systems that store personal data should fall under the jurisdiction of data protection laws or whether exemptions should be made to accommodate the technology's immutable nature.

Another legal paradox arises from blockchain's decentralized and transparent nature. The GDPR and Indonesia's PDP Law mandate that personal data should only be processed for lawful purposes and should not be excessively exposed. However, blockchain, particularly public blockchain networks, functions on a transparent ledger system, where all transactions and stored data are visible to network participants. This level of transparency can create privacy risks, as sensitive information may remain permanently accessible, contradicting data protection laws that require data minimization and the ability to restrict access when necessary.

[55] S M Abd Ali et al., "Redactable Blockchain: Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions," Future Internet 15, no. 1 (2023), https://doi.org/10.3390/fi15010035; E Politou et al., "Privacy in Blockchain," in Learning and Analytics in Intelligent Systems, vol. 26 (2022), https://doi.org/10.1007/978-3-030-85443-0_7; C Wang et al., "Constraints-Based and One-Time Modification Redactable Blockchain," Journal of Internet Technology 24, no. 7 (2023): 1437–46, https://doi.org/10.53106/160792642023122407005.

In permissionless blockchain systems, data is distributed across multiple nodes worldwide, making it difficult to enforce RTBF uniformly. Even if RTBF is upheld in one country, the same data remains accessible through nodes located elsewhere, beyond legal enforcement. This creates a significant jurisdictional challenge, especially considering GDPR's extraterritorial reach and Indonesia's cross-border provisions. Furthermore, Chousein notes that many public blockchains lack mechanisms to ensure GDPR compliance, creating legal uncertainty.[56] Cross-chain redaction also poses challenges, as data changes in one blockchain may require synchronization across others, with complex solutions like IvyRedaction proposed to address this issue.[57]

Blockchain's transnational nature exacerbates enforcement complexities. Both the GDPR (Article 3) and Indonesia's PDP Law (Article 2) apply extraterritorially, extending protections to their respective citizens regardless of where data is processed. However, blockchain data is replicated across nodes globally, making national enforcement mechanisms largely ineffective. Even if RTBF requests are granted by authorities in the EU or Indonesia, the data remains perpetually accessible via nodes in other jurisdictions. This creates "jurisdictional fragmentation," undermining the global enforceability of privacy rights.

Building on this, the RTBF's application in blockchain environments reveals a profound doctrinal challenge. The foundational features of blockchain technology such as immutability, decentralization, and transparency, conflict directly with individual data erasure rights. While blockchain enhances security, auditability, and data integrity, it introduces regulatory tensions in jurisdictions where RTBF is a fundamental right. Drawing on Solove's privacy taxonomy, these conflicts primarily target harms in information dissemination, where persistent data visibility contradicts the legal aim to minimize exposure of outdated or harmful information.[58]

---

[56] Chousein et al., "Tension between GDPR and Public Blockchains: A Data-Driven Analysis of Online Discussions."
[57] S Hu et al., "IvyRedaction: Enabling Atomic, Consistent and Accountable Cross-Chain Rewriting," IEEE Transactions on Dependable and Secure Computing 21, no. 4 (2024): 3883–900, https://doi.org/10.1109/TDSC.2023.3339675.
[58] Daniel J. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review 153, no. 6 (2006): 477–559.

The accountability framework underpinning GDPR and Indonesia's PDP Law relies on the existence of identifiable data controllers and processors, which blockchain disrupts. In the absence of central control, no singular actor bears responsibility for responding to data subject rights, violating basic assumptions of data governance in both jurisdictions. The principle of proportionality further complicates this scenario. While RTBF is not absolute and must be balanced against public interests, blockchain's design challenges the feasibility of this balancing exercise. Public blockchains often serve functions such as financial transparency and fraud prevention, making the outright application of RTBF potentially disruptive to public interests.

In Indonesia, these challenges are compounded by nascent enforcement mechanisms, with limited case law and evolving institutional capacities. This doctrinal gap, exacerbated by blockchain's decentralized nature, signals the need for legal reinterpretation or innovative regulatory adaptations, paving the way for discussion in the next section on potential solutions.

The enforcement of the RTBF within blockchain systems presents a multifaceted regulatory challenge, rooted in the foundational divergence between decentralized technology and traditional privacy frameworks. While both the EU and Indonesia formally recognize RTBF within their data protection regulations, significant doctrinal, regulatory, and institutional obstacles hinder the effective application of RTBF when personal data is recorded on blockchain networks.

Another legal challenge arises from the absence of a clearly identifiable data controller in public, permissionless blockchain environments. The GDPR (Article 4(7)) and Indonesia's PDP Law (Article 1(4)) both rely on the existence of accountable entities—data controllers and processors—responsible for ensuring compliance with privacy rights, including the RTBF. In blockchain networks, particularly decentralized systems such as Bitcoin or Ethereum, no single actor governs or controls the data, resulting in a "regulatory accountability vacuum." This lack of clear accountability makes the practical enforcement of data erasure rights extremely difficult, as no legally responsible party exists to process erasure requests or ensure compliance with judicial

orders. Further reference is recommended here from scholarly discussions on "accountability in decentralized systems."

The study from Koops about “data controller ambiguity” resonates in blockchain environments, where the absence of a centralized entity complicates erasure obligations. This challenge underscores the need for regulatory innovation, such as permissioned, consortium-governed blockchains or off-chain compliance intermediaries, to ensure effective control and potential enforcement of the right to be forgotten.[59]

6. Mechanism to Accommodate RTBF Application and Blockchain’s Immutability and Decentralized Nature

The intersection between the RTBF and blockchain technology presents a significant challenge due to blockchain’s immutable and decentralized nature. This conflict cannot remain unresolved because the absence of a clear resolution risks creating legal uncertainty, undermining both personal data protection and technological innovation of blockchain with immutability nature. A solution is therefore essential to reconcile these principles in a way that upholds the philosophical values embedded in Indonesia’s legal system.

In determining which principle should prevail when conflict of privacy protection under RTBF and blockchain’s immutability nature is unavoidable, the choice must be guided by the philosophical foundation discussed earlier. Pancasila, particularly the second principle (*Just and Civilized Humanity*), emphasizes the protection of human dignity and justice. When the immutability principle of blockchain conflicts irreconcilably with the RTBF, the legal framework should prioritize the protection of individual rights and dignity, while adapting the technical implementation of blockchain to align with this priority. In this context, technological design must yield to legal and ethical imperatives, ensuring that innovation serves, rather than undermines, the human-centered values at the heart of Indonesia’s legal philosophy.

[59] Koops, “Forgetting Footprints, Shunning Shadows. A Critical Analysis of the ‘Right To Be Forgotten’ in Big Data Practice.”

The same rationale applies within the EU, where the GDPR's philosophical basis in the Charter of Fundamental Rights, particularly Articles 7 and 8, prioritizes the protection of human dignity and privacy. In both jurisdictions, when these principles cannot be harmonized, the legal framework must give precedence to individual rights over strict adherence to immutability. In this sense, technological design should adapt to legal and ethical imperatives, ensuring that innovation operates within a framework that upholds human-centered justice.

Therefore, this study proposes solutions through two approaches, first, reinterpretation of RTBF as a "functional right to erasure" consistent with the PDP Law's purpose of making data unidentifiable rather than physically removed. Secondly, technical–legal mechanisms such as key deletion, off-chain storage, and permissioned blockchain. These approaches allow both principles to coexist without eroding the fundamental purposes of either.

6.1. Reinterpretation of the RTBF Regulation and Regulatory Approach

First approach to resolve this conflict involves developing legal interpretation of the RTBF that align with blockchain's unique properties. Koops' classification of RTBF visions—ranging from "deletion in due time" to "clean slate" and "liberty of present expression"[60]—frames the conception that blockchain's immutable structure necessitates a reinterpretation of the right, shifting from traditional physical deletion toward access and control mechanisms that maintain data permanence. This reinterpretation aligns with the broader perspective that, rather than total erasure, privacy protections may need to focus on controlling access and use within an immutable record.

Interpretation is not always limited to the literal meaning or literal language of a provision, but can expand its meaning according to the context and purpose of the law-makers, including in understanding the destruction of personal data, which not only includes physical destruction but also other efforts to eliminate the data's ability to be re-identified.

[60] Ibid.

Regulators can foster blockchain compliance with the Indonesian PDP Law by focusing on shared goals—transparency, data security, and accountability—while reinterpreting traditional legal concepts like "erasure" and "data controllership". Instead of enforcing rigid compliance measures that blockchain cannot technically meet, regulators could establish flexible interpretations and hybrid legal-technical solutions. By doing so, GDPR's objectives of data protection and user empowerment can be upheld without stifling blockchain innovation. [61]

One of the most viable legal strategies for reconciling the RTBF with blockchain's immutable nature is through the doctrinal evolution towards the concept of "right to cryptographic erasure," Cryptographic erasure involves encrypting sensitive data before storage and then deleting the decryption keys when the data needs to be erased. This ensures that the data cannot be accessed or reconstructed without the keys.[62] This concept pivots from the traditional notion of physical erasure towards practical inaccessibility, ensuring that personal data is rendered inaccessible without breaching the structural integrity of the blockchain.

One example is to reinterpret the concept of "destroy" under RTBF in Article 44 of the Indonesia PDP Law. As the explanation of Article 44 of Indonesia's PDP Law states that the erasure means "act of eliminating, erasing, or destructing personal data to the extent that it can no longer be used to identify the data subject." Article 44 also mandates the destruction of personal data upon request. It could be interpreted to allow deletion of cryptographic keys rather than altering blockchain records that contain data directly. This would ensure that data is no longer accessible, achieving the intended effect of RTBF without compromising blockchain's structural integrity.

To accommodate the normative interpretation of the right to cryptographic erasure, Indonesia needs to issue implementing regulations or technical guidelines. These should explicitly address RTBF compliance in decentralized systems, including the use

[61] U Tatar et al., "Law versus Technology: Blockchain, GDPR, and Tough Tradeoffs," Computer Law and Security Review 38 (2020), https://doi.org/10.1016/j.clsr.2020.105454. P. 7 – 8.
[62] A Askarov et al., "Cryptographic Enforcement of Language-Based Information Erasure," Proceedings of the Computer Security Foundations Workshop 2015-September (2015): 334–48, https://doi.org/10.1109/CSF.2015.30.

of key deletion, off-chain storage, or permissioned blockchain. Such targeted refinement would align Indonesia's practice with global standards, provide legal certainty, and fulfill the philosophical foundation of the PDP Law in safeguarding human dignity while supporting lawful technological innovation.

6.2. Hybrid Legal-Technical Solutions

Several hybrid legal-technical mechanisms could operationalize this doctrinal reinterpretation. First, cryptographic key deletion offers a practical solution where access to data is revoked by deleting encryption keys. This achieves functional erasure but remains controversial under GDPR since data technically persists on-chain. However, it is potentially more acceptable within Indonesia's legal framework, which allows broader interpretation of "destroy." Second, off-chain storage enables personal data to be stored outside the blockchain, while only hashes or pointers remain on-chain. This approach supports data minimization and aligns with privacy-by-design principles. Though cautiously welcomed by European regulators, linkability risks must be managed.

Third, another balanced approach is the adoption of permissioned blockchains, which restrict access and control to a defined set of participants. Unlike public blockchains, permissioned systems allow for controlled data management, making it easier to comply with GDPR requirements while maintaining blockchain's efficiency and security.[63] Permissioned blockchains create a semi-centralized structure by limiting access to verified participants, even though, this partially contradicts blockchain's original decentralized philosophy.[64] By introducing centralized control over distributed nodes, modifications can be made when legally required, ensuring compliance with RTBF in the Indonesian PDP Law mandates.

[63] J Sedlmeir et al., "The Transparency Challenge of Blockchain in Organizations," Electronic Markets 32, no. 3 (2022): 1779–94, https://doi.org/10.1007/s12525-022-00536-0.
[64] G M Riva, "What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights," Frontiers in Blockchain 3 (2020), https://doi.org/10.3389/fbloc.2020.00036.

This governance model enables better compliance with erasure requests and data subject rights. It is particularly promising in Indonesia, where regulatory culture is more accustomed to centralized oversight, even though it partially contradicts blockchain's decentralization philosophy. Fourth, advanced cryptographic techniques, including homomorphic encryption and attribute-based encryption, can secure personal data without altering the blockchain structure (64). Nonetheless, these techniques are still in developmental stages, facing scalability and efficiency limitations.

7. Conclusion

The conflict between the RTBF and blockchain's immutability reflects a fundamental challenge in reconciling technological innovation with the protection of individual rights. In both Indonesia and the EU, the RTBF is grounded not only in philosophical principles of human dignity and justice but also in explicit legal foundations. In Indonesia, the RTBF derives its normative legitimacy from Pancasila—particularly the second principle of "Just and Civilized Humanity"—and the 1945 Constitution, especially Articles 28G and 28F, which guarantee protection of personal data and privacy. In the EU, these are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights and codified in Article 17 of the GDPR. These provisions form the doctrinal basis for interpreting the RTBF in light of new technological challenges.

This paper also proposes an interpretation of RTBF application from absolute erasure or the destruction of the data itself to the right of cryptographic erasure, in order to ensure that the data stored on-chain will no longer accessible and identifiable. For Indonesia, fulfilling these philosophical and legal commitments does not necessitate amending the PDP Law itself but requires refinement through implementing regulations and detailed guidance from the authority. Such measures should address RTBF compliance in blockchain contexts, including the use of off-chain storage, and permissioned blockchain, and cryptographic key destruction to make on-chain personal data functionally inaccessible. This approach ensures that the immutable nature of blockchain is preserved in its structural integrity while upholding Indonesia's legal and philosophical mandate to protect human dignity, thus aligning the nation with global best practices while maintaining its character as a rule of law based on Pancasila.

This paper is limited by its doctrinal and comparative method, which does not include empirical validation of the proposed solutions. The analysis is also constrained by the evolving nature of blockchain technology and the lack of binding jurisprudence on RTBF enforcement in blockchain contexts. Therefore, future research should examine the practical feasibility of the "right to cryptographic erasure" through collaboration with technical experts and legal authorities. Comparative studies involving jurisdictions beyond the EU and Indonesia will also be valuable in developing adaptable RTBF–blockchain compliance frameworks.

Acknowledgments

We would like to express sincere gratitude for Indonesia Endowment Fund for Education Agency for the Doctoral Scholarship Awards for the first author of this paper. We also extend gratitude to the Law Science Doctoral Program, Faculty of Law Universitas Gadjah Mada and FORMADIKUM (Doctoral Law Students Forum) of Faculty of Law Universitas Gadjah Mada for the support to publish this paper. We also appreciate reviewers and editors, and any parties involved for their insightful comments, constructive feedback, and valuable suggestions, which have greatly contributed to improving the quality and clarity of this paper.

References

Abd Ali, S M, M N Yusoff, and H F Hasan. "Redactable Blockchain: Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions." *Future Internet* 15, no. 1 (2023). https://doi.org/10.3390/fi15010035.

Abdul-Wadud, A, F A J Osei, S Nurudeen, S Gawusu, and M Abubakar. "Blockchain Technology: Evolution, Potentials, and Operational Challenges." In *The Intersection of Blockchain and Energy Trading: Exploring Decentralized Solutions for Next-Generation Energy Markets*. 2024. https://doi.org/10.1016/B978-0-443-23627-3.00003-X.

Aghili, S. *Leveraging Blockchain Technology: Governance, Risk, Compliance, Security, and Benevolent Use Cases*. In *Leveraging Blockchain Technology: Governance, Risk, Compliance, Security, and Benevolent Use Cases*. 2024. https://doi.org/10.1201/9781003462033.

Al Mashhour, Omar Farouk, Ahmad Shamsul, and Nor Azlina Binti Mohd Noor. "Estate Planning in the Digital Age: Rufadaa as a Lesson to Be Learnt to Improve the Syrian Personal Status Law." *Brawijaya Law Journal* 11, no. 1 (2024): 72–90. https://doi.org/10.21776/ub.blj.2024.011.01.04.

Aljazi, Jehad D. "The Right of Local Government Employees to Expungement of Disciplinary Offences Processed Digitally in Jordanian and Qatari Legislation." *Legality : Jurnal Ilmiah Hukum* 33, no. 1 (2024): 20–43. https://doi.org/10.22219/ljih.v33i1.36212.

Amnesti, Sheila Kusuma Wardani, Siti Zulaichah, and Nurul Istiqomah. "Legal Protection of Personal Data Security in Indonesian Local Government Apps: Al Farabi's Perspective." *Legality : Jurnal Ilmiah Hukum* 33, no. 1 (2024): 1–19. https://doi.org/10.22219/ljih.v33i1.34623.

Andrade, N N G de. "Oblivion: The Right to Be Different … from Oneself: Re-Proposing the Right to Be Forgotten." In *Palgrave Macmillan Memory Studies*. 2014. https://doi.org/10.1057/9781137428455_5.

Anshori, Ahmad Yani, and Landy Trisna Abdurrahman. "Constitutional Contestation of the Islamic State Concept in the Indonesian Parliament 1956-1959." *De Jure: Jurnal Hukum Dan Syar'iah* 16, no. 2 (2024): 278–316. https://doi.org/10.18860/j-fsh.v16i2.29572.

Anwar, F, B U I Khan, M.L.B.M. Kiah, N A Abdullah, and K W Goh. "Comprehensive Insight into Blockchain Technology: Past Development, Present Impact and Future Considerations." *International Journal of Advanced Computer Science and Applications* 13, no. 11 (2022): 878–907. https://doi.org/10.14569/IJACSA.2022.01311101.

Arief Budiman, Muhammad Saifullah, and Bahrul Ulum. "Wājibah Will for Non-Muslim Heirs in Indonesia: A Legal Political Perspective Based on Justice and Welfare." *Ijtihad : Jurnal Wacana Hukum Islam Dan Kemanusiaan* 24, no. 2 (2024): 223–50. https://doi.org/10.18326/ijtihad.v24i2.223-250.

Askarov, A, S Moore, C Dimoulas, and S Chong. "Cryptographic Enforcement of Language-Based Information Erasure." *Proceedings of the Computer Security Foundations Workshop* 2015-September (2015): 334–48. https://doi.org/10.1109/CSF.2015.30.

Baets, A De. "A Historian's View on the Right to Be Forgotten." *International Review of Law, Computers and Technology* 30, nos. 1–2 (2016): 57–66. https://doi.org/10.1080/13600869.2015.1125155.

Chakim, Lutfi, Nur Hidayah, and Hasanudin Hasanudin. "Fatwa, Authority, and Digital Trade: A Critical Legal-Discursive Analysis of Dropshipping Rulings in Indonesia and Egypt." *Jurisdictie: Jurnal Hukum Dan Syariah* 16, no. 1 (2025): 124–65. https://doi.org/10.18860/j.v16i1.31882.

Chen Siqi, Ramalinggam Rajamanickam, Nazura Abdul Manap, and Zamre Mohd Zahir. "Application of Blockchain Technology in Cross-Border Telecommunications Network Fraud to Ensure China's Judicial Justice." *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 3 (2024): 472–86. https://doi.org/10.29303/ius.v12i3.1554.

Chousein, Z, H Y Tetik, R B Saglam, A Bülbül, and S Li. "Tension between GDPR and Public Blockchains: A Data-Driven Analysis of Online Discussions." *ACM International Conference Proceeding Series*, 2020. https://doi.org/10.1145/3433174.3433587.

Daniel J. Solove. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 153, no. 6 (2006): 477–559.

Devisri, M, V Vetriselvan, M Baskar, M Mylapalli, S K M Kolluru Mouli, and K Jayabalan. "Blockchain Innovations for Secure Online Transactions." In *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning*. 2024. https://doi.org/10.4018/979-8-3693-6557-1.ch021.

Gavalas, Modestos. "Does Blockchain Technology Per Se Constitute a Breach of the GDPR? An Effort to Harmonize Two Seemingly Opposing Concepts." *Global Privacy Law Review* (Alphen aan den Rijn, The Netherlands), Kluwer Law International, 2025, 66–72.

Grafenstein, M Von, and W Schulz. "The Right to Be Forgotten in Data Protection Law: A Search for the Concept of Protection." *International Journal of Public Law and Policy* 5, no. 3 (2015): 249–69. https://doi.org/10.1504/IJPLAP.2015.075049.

Hu, S, M Li, J Weng, J.-N. Liu, J Weng, and Z Li. "IvyRedaction: Enabling Atomic, Consistent and Accountable Cross-Chain Rewriting." *IEEE Transactions on Dependable and Secure Computing* 21, no. 4 (2024): 3883–900. https://doi.org/10.1109/TDSC.2023.3339675.

Imam, M, and K Saini. "A Review of Applications and Security: Blockchain Technology." In *Blockchain and EHR*. 2024.

Jambert, A. "Blockchain and the GDPR: A Data Protection Authority Point of View." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11469 LNCS (2019): 3–6. https://doi.org/10.1007/978-3-030-20074-9_1.

Jones, M L, E Zeide, J.-E. Mai, E Jones, J Dupre, and N Richards. "The Right to Be Forgotten." *Proceedings of the Association for Information Science and Technology* 52, no. 1 (2015): 1–3. https://doi.org/10.1002/pra2.2015.145052010010.

Kelly, M J, and D Satola. "The Right to Be Forgotten." *University of Illinois Law Review* 2017, no. 1 (2017): 1–64.

Kemenkumham. "Naskah Akademik RUU Perlindungan Data Pribadi." *Kementerian Hukum Dan Hak Asasi Manusia*, 2022, 121.

Koops, Bert-Jaap. "Forgetting Footprints, Shunning Shadows. A Critical Analysis of the 'Right To Be Forgotten' in Big Data Practice." *SCRIPTed* 8, no. 3 (2011): 1–28. https://doi.org/10.2966/scrip.

Kumar, D K, N Duraimutharasan, H J Shanthi, G Vennila, B Prabu Shankar, and P Senthil. "Comparative Analysis of Transaction Speed and Throughput in Blockchain and Hashgraph: A Performance Study for Distributed Ledger Technologies." *Journal of Machine and Computing* 3, no. 4 (2023): 497–504. https://doi.org/10.53759/7669/jmc202303041.

Leiser, M R. "'Private Jurisprudence' and the Right to Be Forgotten Balancing Test." *Computer Law and Security Review* 39 (2020). https://doi.org/10.1016/j.clsr.2020.105458.

Liu, Q, and J Shen. "K-Time Redactable Blockchain with Decentralized History Rewriting." *Proceedings - 2023 International Conference on Data Security and Privacy Protection, DSPP 2023*, 2023, 41–49. https://doi.org/10.1109/DSPP58763.2023.10404463.

Mach, M. "The Right to Be Forgotten in Response to the Development of Information Technology." *Pravnik* 160, no. 7 (2021): 597–609.

Moondra, R, V Sihag, and G Choudhary. "EthFor: Forensic Investigation Framework for Ethereum Blockchain." *Lecture Notes in Networks and Systems* 765 LNNS (2023): 481–88. https://doi.org/10.1007/978-981-99-5652-4_43.

Mukherjee, P, and C Pradhan. "Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology." In *Intelligent Systems Reference Library*, vol. 203. 2021. https://doi.org/10.1007/978-3-030-69395-4_3.

Oganesian, T D. "Legal Framework, Limits and Standards for the Application of the Right to Be Forgotten: The Experience of the European Union." *Vestnik Sankt-Peterburgskogo Universiteta. Pravo* 14, no. 3 (2023): 750–67. https://doi.org/10.21638/spbu14.2023.312.

Parikh, Anand Manojkumar, Shamik Sural, Vijayalakshmi Atluri, and Jaideep Vaidya. "Enabling Right to Be Forgotten in a Collaborative Environment Using Permissioned Blockchains." In *Data and Applications Security and Privacy XXXIX*, edited by Sokratis Katsikas and Basit Shafiq. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-96590-6_9.

Politou, E, E Alepis, M Virvou, and C Patsakis. "Privacy in Blockchain." In *Learning and Analytics in Intelligent Systems*, vol. 26. 2022. https://doi.org/10.1007/978-3-030-85443-0_7.

Ria Setyawati, Stefan Koos, and Zalfa A.F. Jatmiko. "Data Driven Dominance in Digital Markets: Assessing Indonesian Competition Law in the Digital Age." *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 2 (2024): 264–84. https://doi.org/10.29303/ius.v12i2.1377.

Riva, G M. "What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights." *Frontiers in Blockchain* 3

(2020). https://doi.org/10.3389/fbloc.2020.00036.

Sartor, G. "The Right to Be Forgotten: Balancing Interests in the Flux of Time." *International Journal of Law and Information Technology* 24, no. 1 (2016): 72–98. https://doi.org/10.1093/ijlit/eav017.

Sedlmeir, J, J Lautenschlager, G Fridgen, and N Urbach. "The Transparency Challenge of Blockchain in Organizations." *Electronic Markets* 32, no. 3 (2022): 1779–94. https://doi.org/10.1007/s12525-022-00536-0.

Setyardi, Heribertus Untung. "Right To Be Forgotten Vis-À-Vis Hak Atas Informasi." *Jurnal Kewarganegaraan* 8, no. 1 (2024): 1096–108. https://doi.org/10.31316/jk.v8i1.6529.

Shah, J, and S Parveen. "Understanding the Blockchain Technology Beyond Bitcoin." *Lecture Notes in Mechanical Engineering*, 2021, 499–516. https://doi.org/10.1007/978-981-33-4320-7_45.

Sharma, S, O Sharma, and J Arora. "Consensus Mechanisms Analysis: A Remedy for the Byzantine Generals Problem." *Proceedings - International Conference on Technological Advancements in Computational Sciences, ICTACS 2023*, 2023, 674–78. https://doi.org/10.1109/ICTACS59847.2023.10390006.

Sobkow, B. "Forget Me, Forget Me Not - Redefining the Boundaries of the Right to Be Forgotten to Address Current Problems and Areas of Criticism." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10518 LNCS (2017): 34–51. https://doi.org/10.1007/978-3-319-67280-9_3.

Sriono, Risdalina, Kusno, Indra Kumalasari M, and Hengki Syahyunan. "Legal Protection for Digital Bank Customers in Indonesia: Analysis of Data Confidentiality Regulations and Bank Responsibility." *LITIGASI* 25, no. 2 (2024): 301–30. https://doi.org/10.23969/litigasi.v25i2.18538.

Stacy Ogechukwu Ikemefuna-Amaechi. "Balancing Privacy and Innovation: Exploring the Conflict Between Data Protection Rights and Blockchain's Immutability and Decentralized Nature." In *Master's Thesis in EU Law, with a Specialization in Data Protection Law*. Uppsala Universitet, 2025.

Stoddart, J. "Lost in Translation: Transposing the Right to Be Forgotten from Different Legal Systems." In *The Right to Be Forgotten: A Canadian and Comparative Perspective*. 2020. https://doi.org/10.4324/9781003017011-2.

Suripeddi, M K S, and P Purandare. "Blockchain and GDPR - A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing." *Journal of Physics: Conference Series* 1964, no. 4 (2021). https://doi.org/10.1088/1742-6596/1964/4/042005.

Suryahartati, Dwi, Windarto, and Lestari. "Tradisi Hukum Dan Inovasi Digital: Menakar

Posisi Produk E- Notary Pada Sengketa Perdata: Legal Tradition and Digital Innovation: Assessing the Position of e-Notary Products in Civil Disputes." *LITIGASI* 26, no. 1 (2025): 409–47. https://doi.org/10.23969/litigasi.v26i1.19193.

Tatar, U, Y Gokce, and B Nussbaum. "Law versus Technology: Blockchain, GDPR, and Tough Tradeoffs." *Computer Law and Security Review* 38 (2020). https://doi.org/10.1016/j.clsr.2020.105454.

Tejomurti, Kukuh, Sukarmi Sukarmi, Budi Santoso, and Hanif Nur Widhiyanti. "Big Data Analytics Algorithms for Dynamic Pricing: The Legal Analysis of the Indonesia Competitions Law Readiness in Digital Era." *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 1 (2024): 68–90. https://doi.org/10.29303/ius.v12i1.1303.

Thilakavathy, P, S Jayachitra, A Aeron, N Kumar, S S Ali, and M Malathy. "Investigating Blockchain Security Mechanisms for Tamper-Proof Data Storage." *2023 International Conference on Communication, Security and Artificial Intelligence, ICCSAI 2023*, 2023, 926–30. https://doi.org/10.1109/ICCSAI59793.2023.10421006.

Vavra, A N. "The Right to Be Forgotten: An Archival Perspective." *American Archivist* 81, no. 1 (2018): 100–111. https://doi.org/10.17723/0360-9081-81.1.100.

Wang, C, Y Chen, and W Jia. "Constraints-Based and One-Time Modification Redactable Blockchain." *Journal of Internet Technology* 24, no. 7 (2023): 1437–46. https://doi.org/10.53106/160792642023122407005.

Wang, G, and M Nixon. "SoK: Essentials of BFT Consensus for Blockchains." *2023 5th International Conference on Blockchain Computing and Applications, BCCA 2023*, 2023, 315–28. https://doi.org/10.1109/BCCA58897.2023.10338868.

Wang, G, and M Nixon. "SoK: X-Assisted BFT Consensus Protocols." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 14206 LNCS (2023): 54–71. https://doi.org/10.1007/978-3-031-44920-8_4.

Wang, H, H Ning, Y Lin, et al. "A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges." *IEEE Internet of Things Journal* 10, no. 16 (2023): 14671–88. https://doi.org/10.1109/JIOT.2023.3278329.