Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966

Volume VI, Nomor 1,
Juli, 2025

FROM PRIVACY TO OBLIVION: THE RIGHT TO BE FORGOTTEN IN INDONESIA'S SOCIAL MEDIA PLATFORMS

Shinta Kumala Syari[1], Sahat Parlindungan Simarmata[2], Khairina Widyanti[3], Stefani Nuranugrah Putrijaya[4]

Universitas Pelita Harapan
Jalan M.H. Thamrin Boulevard No.1100, Kelapa Dua, Tangerang Regency, Banten 15811
Email: 01053240063@student.uph.edu[1]; 01053240086@student.uph.edu[2]; 01053240087@student.uph.edu[3]; 01053240077@student.uph.edu[4];

ABSTRACT

The growing permanence of personal information on social media platforms has created an urgent demand for enhanced legal safeguards for digital identities, especially through mechanisms that allow individuals to request the removal of their data. This is acknowledged in Law No. 27/2022 on Personal Data Protection, its practical implementation within the context of social media still faces significant legal challenges. This article examines how the right to be forgotten is interpreted and operationalized within the social media ecosystem in Indonesia, focusing on platform responsibility and the limitations of user control over their personal data. Through doctrinal legal analysis and socio-legal document review, this article explores the normative scope and real-world application of the right to be forgotten, comparing it with the more established legal guidelines in the European Union. The findings indicate that while there is recognition of the principle of digital erasure, users often find themselves trapped in opaque policies and procedural uncertainties. This article proposes policy recommendations to strengthen user rights, enhance regulatory clarity, and harmonize cross-border enforcement in the digital age.

Keywords*: right to be forgotten, Indonesia, digital erasure, social media, platform responsibility, Personal Data Protection Law, data protection, digital rights enforcement*

1. Introduction

In the current digital era, an individual's public identity is often shaped and influenced by the digital footprint they leave on social media.[1] Nowadays, social media has become an archive of collective memory where every content, once shared, can resurface, be reinterpreted, and circulate indefinitely. This phenomenon presents new challenges related to privacy and reputation, as individuals strive to manage their public image.[2] One developing idea in this area is the notion of allowing individuals to have their personal information removed from the internet, especially when such data could harm their reputation.[3]

[1] Feher, Katalin. "Digital identity and the online self: Footprint strategies - An exploratory and comparative research study." *Journal of information science* 47, no. 2 (2021): 192-205.
[2] Liu, Chi, Tianqing Zhu, Jun Zhang, and Wanlei Zhou. "Privacy intelligence: A survey on image privacy in online social networks." *ACM Computing Surveys* 55, no. 8 (2022): 1-35.
[3] Acquisti, Alessandro. "The economics of personal data and the economics of privacy." *Economics* 11 (2010): 24.

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

This study focuses on the transformation of the public identity of Kartika Putri, an Indonesian celebrity who decided to wear hijab and remove her previous non-hijab photos from social media. This decision not only reflects her spiritual journey but also highlights how individuals can attempt to control their public narratives in the digital world. In this context, the support from netizens advocating for the removal of Kartika's old photos demonstrates a collective awareness of the importance of respecting individual decisions in shaping their identities.

For instance, the experience of an influencer who faced negative repercussions from old photos posted on social media is also relevant. After experiencing bullying and public pressure, the influencer requested the removal of certain photos deemed harmful to their reputation.[4] This case, like that of Kartika Putri, illustrates the challenges individuals face in managing their digital footprints and how the concept of the right to be forgotten can provide them with the space to alter existing narratives.

Although the normative foundation of this right is rooted in personal autonomy and privacy protection, its application within the social media landscape, as characterized by virality, user interactivity, and platform autonomy, has revealed complex legal tensions that remain unresolved. Previous research has drawn attention to the philosophical basis and legal complexities of this right.[5] Carnegy-Arbuthnott argues that what is often framed as a privacy issue actually reflects deeper concerns about reputational distortion, particularly when outdated yet true information is recontextualized through search engines or social media in ways that jeopardize an individual's self-presentation.[6] His analysis shifts the legal discourse from mere privacy to a broader taxonomy of rights, including claims against defamation and distortion that are especially critical in cases where platform algorithms elevate irrelevant past data to public visibility.

Complementing this, Sadovska (2022) offers an extensive legal-historical examination of how the concept of data removal emerged as a reaction to the enduring nature of digital content. She identifies three typologies of removal requests: self-posted content removal, reposted content removal, and user-generated content about others, all of which become legally and technically convoluted within the social media ecosystem.[7] Importantly, Sadovska highlights the fragmented global legal responses and strong resistance from technology platforms, particularly in interpreting and applying the balance between freedom of expression and digital removal.

These insights collectively reveal critical gaps in the current regulatory landscape: while the General Data Protection Regulation ("**GDPR**") and court rulings like Google Spain SL v. AEPD[8] have

[4] Valenzuela-García, Noelia, Diego J. Maldonado-Guzmán, Andrea García-Pérez, and Cristina Del-Real. "Too lucky to be a victim? An exploratory study of online harassment and hate messages faced by social media influencers." *European journal on criminal policy and research* 29, no. 3 (2023): 397-421.

[5] Williams, Andrew T. "Taking values seriously: Towards a philosophy of EU law." *Oxford Journal of Legal Studies* 29, no. 3 (2009): 549-577.

[6] Carnegy-Arbuthnott, Hannah Maeve. "Privacy, publicity, and the right to be forgotten." *Journal of Political Philosophy* (2023).

[7] *Sadovska*, Diana. "The Right To Be Forgotten: Establishment And Development." Visnyk of the Lviv University. Series Law 74, no. 74 (June 30, *2022*): 68–78.

[8] The Court of Justice of the European Union ruled that search engines like Google are data controllers and must remove links to personal information when it is outdated, irrelevant, or excessive, even if the original content is lawful. This decision arose from a complaint by Mario Costeja González, who wanted links to a 1998 article about his past debts removed. The ruling emphasized individuals' rights to privacy and data protection under EU law and laid the groundwork for the right to erasure in the GDPR. (Court of Justice of the European Union. (2014). Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131)

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

established basic protections, enforcement mechanisms - especially within the context of social media - remain inconsistent, unclear, and largely dependent on the discretion of platform providers. Many platforms, although classified as data controllers, evade accountability by exploiting jurisdictional fragmentation or embedding user agreements that prioritize corporate interests over individual rights.[9]

The issue is exacerbated by technical realities: viral content, reshared media, and algorithmically preserved interactions challenge the feasibility of digital removal. As noted by Carnegy-Arbuthnott, deleting search links does not remove content from its source, nor does it mitigate reputational harm amplified by digital curation.[10] Similarly, Sadovska emphasizes that mere legal recognition is insufficient without coherent international enforcement and technical collaboration from platforms.[11]

The urgency of this legal discourse is underscored by the accelerating disclosure of personal data on social media platforms and the increasing normalization of algorithmic permanence. In recent years, the misuse and uncontrolled circulation of sensitive user content, ranging from embarrassing teenage posts to past legal issues, have triggered reputational damage, cyberbullying, and long-term exclusion from educational, professional, or financial opportunities.[12] Although removal features are often presented as tools for user empowerment, these features are frequently superficial; deleted uploads from user accounts may still exist in shared content, screenshots, third-party archives, or reappear through automated search indexing. Furthermore, the integration of social media with biometric data, geolocation tracking, and metadata collection means that users rarely have meaningful control over the removal of their digital footprints.[13]

This situation has created a serious crisis of consent and asymmetry between user expectations of privacy and the storage and dissemination practices of platforms. Compounding this issue is the inconsistent implementation of removal requests and the absence of integrated procedural protections. Most major platforms offer non-binding and discretionary removal processes that often lack transparency, appeal mechanisms, or accountability benchmarks.[14] Users frequently encounter delays, unclear rejections, or partial removals, especially when content is deemed to serve the "public interest," a term that is undefined and often arbitrarily interpreted.

In a cross-border context, this issue deepens; users protected under jurisdictions like the European Union theoretically possess removal rights, but enforcement becomes shaky when content is hosted or managed in countries with limited or no protections at all.[15] This fragmentation enables

[9] Gawankar, Yash, and Srinivas Naik. "Anticipating the Evolution of Data Accountability through Technological Advancements and Regulatory Landscape Changes." In *Cloud Security*, pp. 143-159. Chapman and Hall/CRC, 2024.

[10] Carnegy-Arbuthnott, Hannah Maeve. "Privacy, publicity, and the right to be forgotten." *Journal of Political Philosophy* (2023).

[11] ibid. Sadovska., hal. 70

[12] Beg, Rijvan, Vivek Bhardwaj, Mukesh Kumar, Prathamesh Muzumdar, Aman Rajput, and Kamal Borana. "Unmasking Social Media Crimes: Types, Trends, and Impact." *Online Social Networks in Business Frameworks* (2024): 1-26.

[13] Muhammad, Syed Sardar, Bidit Lal Dey, and Vishanth Weerakkody. "Analysis of factors that influence customers' willingness to leave big data digital footprints on social media: A systematic review of literature." *Information Systems Frontiers* 20 (2018): 559-576.

[14] Park, Tae Jung, and Akshita Rohatgi. "Balancing the platform responsibility paradox: A case for amplification regulation to mitigate the spread of harmful but legal content online." *Computer Law & Security Review* 52 (2024): 105960.

[15] Parti, Katalin, and Luisa Marin. "Ensuring freedoms and protecting rights in the governance of the internet: A comparative analysis on blocking measures and internet providers' removal of illegal internet content." *Journal of Contemporary European Research* 9, no. 1 (2013).

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

multinational platforms to forum shop or selectively invoke freedom of expression defenses, undermining the universality of digital rights. Another pressing concern is the increasing reputational surveillance and data persistence technologies used by employers, insurance companies, and state actors, who utilize social media content in profiling, risk assessment, and decision-making processes.

Without strong and enforceable removal rights, users are exposed to long-term consequences based on content that may be outdated, misrepresentative, or contextually misunderstood. The commodification of user data further discourages platforms from cooperating with removal requests, as archival data becomes input for machine learning models, targeted advertising, and behavioral predictions. In such an environment, the lack of comprehensive and enforceable legal obligations on platforms not only erodes individual dignity but also diminishes democratic values such as the right to reform, rehabilitate, and move forward without being burdened by one's digital past.

This research is driven by the urgent need to interrogate and refine the legal responsibilities of social media platforms concerning digital removal. The study aims to explore the doctrinal, procedural, and normative complexities surrounding the concept of data erasure in this unique context. Specifically, it will examine the legal status of platforms as data controllers, existing legal limitations on data protection in the transnational digital space, and the role of public interest and freedom of expression as balancing factors in personal removal claims. By focusing on platform responsibilities and the enforceability of digital removal, this research seeks not only to bridge existing legal gaps but also to propose pragmatic reforms that strengthen individual agency in an era where forgetting is no longer a natural process but also a battleground of law and technology.

2. Research Methodology

This study employs a qualitative legal approach based on two complementary methods: doctrinal legal analysis and socio-legal document analysis. These methods were chosen to critically examine how the right to be forgotten is constructed, interpreted, and enforced within the framework of digital privacy legislation, particularly in the context of social media platform responsibilities regarding digital erasure.

Doctrinal Legal Analysis method is utilized to conduct a systematic study of the regulations, legal principles, and judicial interpretations related to the concept of data removal, specifically within the context of Indonesian legislation and its comparison with the GDPR. The focus of the analysis will include how Article 15 of the Personal Data Protection Law No. 27/2022 ("PDP Law") in Indonesia is interpreted in real cases, such as the case of Kartika Putri, as well as the legal obligations imposed on social media platforms in processing data erasure requests.

The primary method employed is doctrinal legal analysis, which involves a systematic study of laws, legal principles, and judicial interpretations as found in authoritative legal sources. This method enables the researcher to investigate the normative basis of the right to be forgotten, as outlined in Article 17 of the GDPR, and to assess its contextualization within wider human rights frameworks, including the Charter of Fundamental Rights of the European Union.

This analysis focuses on identifying the legal obligations imposed on digital platforms as data controllers, the exceptions applicable to erasure claims, and the interpretive inconsistencies that arise in the application of the law. This doctrinal foundation provides the necessary legal grounding to

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

assess whether existing laws and precedents offer adequate protection for users seeking digital erasure of their personal information on social media.

Complementing this normative legal examination is the socio-legal analysis of documents, which considers specific rulings from the Court of Justice of the European Union ("**CJEU**") obtained from the official CURIA database as empirical evidence. These judicial documents are analyzed thematically to uncover the factual context, legal arguments presented by the claimant and the platform, and the court's considerations in balancing the right to privacy with public interest and freedom of expression. Beyond its doctrinal content, this case is interrogated for its social and procedural implications, particularly regarding how legal rights are operationalized in real disputes and how this affects users' lived experiences.

Through this lens, the study explores whether court decisions have successfully clarified platform responsibilities or, conversely, may have inadvertently reinforced ambiguities in legal enforcement and accountability. This method will also involve an in-depth analysis of the Kartika Putri case as an empirical case study. The research will explore the factual context behind Kartika's decision to delete her photos, including netizen reactions and the social impact of the erasure. It will also include an analysis of how social media platforms handle erasure requests and the challenges users face in this process.

These two methodological approaches allow for a holistic examination of data privacy rights and RTBF as both a legal principle and a contested practice within the digital environment. The doctrinal analysis ensures rigorous legal interpretation, while the socio-legal document analysis grounds the research in real-world judicial developments. This methodological synthesis enables the study not only to map the legal landscape but also to offer a reasoned critique of its limitations, ultimately supporting a normative argument for stronger, coherent, and enforceable digital erasure mechanisms in the realm of online platforms.

3. Research Findings and Discussion

The findings of this research underscore the inherent tension between the normative aspirations of data erasure rights and the practical realities of enforcing this right within the social media ecosystem. Doctrinally, Article 17 of the GDPR provides a robust framework for individual digital autonomy by allowing individuals to request the removal of personal information on specific legal grounds. However, this rights structure is laden with exceptions, requirements, and balancing tests that expose legal ambiguities that can be exploited by platforms. While the regulation mandates data controllers to act "without undue delay," it simultaneously permits them to deny requests on the grounds of freedom of expression, public interest, or legal obligation, often without clear thresholds or procedural transparency. This inherent discretion disproportionately benefits large digital platforms, which can utilize broad interpretations of public relevance and request procedural delays that render the removal process ineffective or inaccessible to ordinary users.

A socio-legal analysis of selected CJEU case documents illustrates how these doctrinal tensions play out in judicial practice. The chosen rulings not only affirm the principle of digital removal but also reveal the cautious and often conservative stance of the judiciary in delineating platform responsibilities. While the courts acknowledge the legitimate interests of plaintiffs seeking the removal of outdated or reputationally harmful information, they concurrently reinforce the need to assess each

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

case through a contextual lens that involves the individual's role in public life, the accuracy of the information, and the temporal relevance of the content. Consequently, the courts leave platforms with a broad margin of interpretative freedom, particularly in determining whether the content remains within the "public interest." This creates procedural and epistemic burdens for users, who are rarely equipped to formulate legally persuasive arguments or effectively challenge platform rejections.

Moreover, the rulings reflect a broader trend in digital jurisprudence where courts recognize platform accountability in theory but avoid imposing enforceable direct obligations that could alter the structural design or business models of these platforms. The absence of binding procedural standards regarding how platforms should evaluate and process removal requests contributes to systemic ambiguity. Users often remain unaware of their rights, the status of their requests, or the reasons for rejections. Dependence on opaque internal decision-making mechanisms controlled by platforms further erodes the position of users as rights-bearing subjects. This matter goes beyond mere privacy issues; it fundamentally revolves around a person's right to manage the representation of their online identity, unhindered by the continuous emergence of obsolete or negative information.

Sadovska's (2022) typology of removal scenarios, i.e.,self-posted content, reposted content, and third-party generated content, highlights the doctrinal and procedural inconsistencies within the existing regulatory regime.[16] The GDPR does not provide distinct enforcement strategies for these various content sources, leading to disparate outcomes depending on how and where data was originally shared.[17] This research finds that social media platforms often treat removal requests homogenously, applying blanket policies that overlook these nuances. This not only undermines the extent of protection under the right to privacy but also forces users to navigate a fragmented system lacking meaningful interpretative guidance and avenues for redress.[18]

Based on these findings, this research argues that the current judicial interpretations, while symbolically significant, do not adequately protect users in practice. The platform-centric architecture of digital memory, characterized by algorithmic curation, archival persistence, and content virality, demands more than mere recognition of user rights; it necessitates the imposition of affirmative obligations on platforms to ensure that these rights can be enforced both technically and procedurally.[19] Courts and regulators must move beyond abstract balancing to establish concrete procedural protections, such as mandatory response timelines, appeal mechanisms, and independent oversight of the removal process. Absent such systemic reforms, the RTBF risks becoming a performative legal framework, recognized on paper but unfulfilled in practice.

The GDPR from the European Union is widely regarded as the most thorough legal framework for personal data protection globally, prominently featuring a well-defined right to data deletion in Article 17.[20] Conversely, Indonesia's newly implemented Personal Data Protection Law No. 27 of 2022

[16] ibid. Sadovska., hal 73

[17] Gal, Michal S., and Oshrit Aviv. "The competitive effects of the GDPR." *Journal of Competition Law & Economics* 16, no. 3 (2020): 349-391.

[18] Inam Ul Mansoor, Sheikh. "An Interface between Digital Privacy and Human Rights: The Challenges Ahead." *Available at SSRN 5019128* (2023).

[19] Ringel, Sharon, and Rivka Ribak. "Platformizing the past: The social media logic of archival digitization." *Social Media+ Society* 10, no. 1 (2024): 20563051241228596.

[20] Schwerin, Simon. "Blockchain and privacy protection in the case of the european general data protection regulation (GDPR): a delphi study." *The Journal of the British Blockchain Association* 1, no. 1 (2018).

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

also acknowledges this right, though it does so in a more general and developing manner.[21] This analysis demonstrates that, while both legal systems emphasize digital privacy and individual autonomy, there are marked differences in their legal frameworks, clarity of procedures, and enforcement methods, especially in the context of social media.

The GDPR articulates the right to be forgotten with clear legal criteria. Article 17 empowers individuals to request the deletion of their personal data under various conditions, such as when the data is no longer essential for its initial purpose, when consent has been revoked, or when the data has been unlawfully processed. Notably, the GDPR specifies circumstances under which data controllers may deny deletion requests, including considerations for freedom of expression, public interest, or compliance with legal obligations.[22] Although these provisions are often subject to debate regarding their implementation, they come with comprehensive procedural requirements for platforms, encompassing notification responsibilities, principles of accountability, and avenues for seeking redress through data protection authorities. The case law from the CJEU further interprets these rights, granting platforms significant latitude in uncertain situations.[23]

In comparison, Indonesia's PDP Law recognizes the right to data deletion in Article 8 and Article 9, which allows individuals to request the deletion or destruction of their data under specific circumstances. However, the Indonesian legislation lacks a detailed framework for this right. given that the implementing regulation is still under harmonization and has yet to be finalized. Currently, here is no explicit procedural guideline outlining how and when data controllers, especially those operating social media platforms, should handle deletion requests.[24] While the PDP Law grants individuals the right to erasure, the absence of implementing regulations leaves significant ambiguity in its enforcement. Moreover, the PDP Law lacks clarity regarding exceptions, such as public interest or freedom of information. as of mid-2015, Indonesia has not yet established an independent data protection authority, similar to the Data Protection Authorities (DPAs) in the EU.[25] This absence of institutional support significantly undermines law enforcement and limits users' recourse options in cases of non-compliance or platform misconduct.

One key difference lies in the scope and enforcement of platform accountability. Under the GDPR, social media companies are explicitly designated as data controllers, with binding obligations to respond to deletion requests in a timely, reasoned, and transparent manner.[26] Administrative fines for non-compliance can reach up to 4% of global annual revenue, creating strong incentives for compliance. On the other hand, while the PDP Law adopts similar terminology of "data controllers"

[21] Prastyanti, Rina Arum, and Ridhima Sharma. "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India." *Journal of Human Rights, Culture and Legal System* 4, no. 2 (2024): 354-390.

[22] Brimblecombe, Fiona. "The public interest in deleted personal data? The right to be forgotten's freedom of expression exceptions examined through the lens of Article 10 Echr." *Journal of Internet Law* 23, no. 10 (2020): 1-29.

[23] Anagnostopoulou, Despina. "The Role of the Court of Justice of the European Union on the Interpretation of Platform Operators and Business Users' Contracts." In *Quo vadis Commercial Contract? Reflections on Sustainability, Ethics and Technology in the Emerging Law and Practice of Global Commerce*, pp. 33-82. Cham: Springer International Publishing, 2023.

[24] Minaei, Mohsen, S. Chandra Mouli, Mainack Mondal, Bruno Ribeiro, and Aniket Kate. "Deceptive deletions for protecting withdrawn posts on social media platform." In *NDSS*. 2021.

[25] Gomes, Sofia Mira Pereira Jesus. "EU personal data protection standards beyond its borders: An analysis of the european external governance through GDPR on Data Protection Laws in the ASEAN region." Master's thesis, 2024.

[26] Jonasson, Fredrik. "A system for GDPR-compliant collection of social media data: from legal to software requirements." (2019).

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

and "data processors," its enforcement regime is still under development. Although the PDP Law provides for both administrative and criminal sanctions under Article 57 and Articles 67-73, the absence of implementing regulations and institutional infrastructure limits the effectiveness of enforcement. This creates uncertainty for users and platforms, particularly for transnational platforms that may choose to comply with the laws of their home jurisdictions rather than Indonesian law.

Another important distinction is in procedural transparency and user empowerment. The GDPR mandates clear communication, avenues for appeal, and access to compensation, whereas the current Indonesian framework does not yet specify how users can monitor, object to, or escalate unresolved deletion requests.[27] In practice, this means that users in Indonesia may face greater barriers to effectively exercising their deletion rights, especially when dealing with global platforms that prioritize compliance with jurisdictions imposing stricter penalties.

Conflicts Between the Right to be Forgotten and Freedom of Expression

Article 17 of the GDPR defines the right to be forgotten as the right of the data subject to obtain the deletion of irrelevant personal data concerning him/her without delay from the data controller and the data controller is obliged to delete personal data without indefinite delay. The concept of right to be forgotten was then adopted into the Indonesian legal system through the revision of Law No. 11 of 2008 concerning Information and Electronic Transactions which was later ratified as Law No. 19 of 2016 as amended by Law No. 1 of 2024.[28]

The obstacles to the implementation of the right to be forgotten in the context of Indonesian law are formulated in the phrase "the right to the deletion of irrelevant (personal) information". The discussion related to the regulation of the right to be forgotten itself is closely related to the personal rights and privacy rights of a person, which means that personal data must be maximized by the state. In short, the provisions in Article 26 of the Revised Electronic Transaction Information Law Number 19 of 2016 provide provisions for the protection of a person's personal data, where a person whose rights have been violated can file a lawsuit with the Court regarding a case that is detrimental to one of the parties due to the dissemination of his/her personal data. Based on the provisions in Article 26 Paragraph (1) of the Revised Electronic Transaction Information Law (UU ITE), the use of any information related to a person's personal data in electronic media, to disseminate the information must have the consent of the person. However, if this is violated, the person concerned can file a lawsuit in accordance with the provisions of Article 26 Paragraph (2) of the Revised Electronic Transaction Information Law (UU ITE).[29] However, this is limited by something that the public must know.

These legal and procedural gaps become particularly evident in real-world cases, such as that of Kartika Putri. Her experience highlights the fundamental conflicts between the right to be forgotten and the principle of freedom of expression, especially regarding social media. Although the right to be forgotten seeks to shield individuals from the detrimental effects of obsolete or harmful content, it frequently clashes with the public's interest in obtaining information. Kartika Putri's decision to delete

[27] Satwiko, Brahmantyo Suryo. "Privacy and data protection: Indonesian legal framework." *Corporate and Trade Law Review* 1, no. 2 (2021): 98-118.

[28] Politou, Eugenia, Efthimios Alepis, Maria Virvou, and Constantinos Patsakis. *Privacy and data protection challenges in the distributed era*. Vol. 26. Cham: Springer, 2022.

[29] Karunia Fitri Rahmadani and M. Darin Arif Mu'allifin, "Legal Analysis of the Regulation of the Right to Be Forgotten in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions", Legacy: Journal of Law and Legislation Vol 3 No.1-March, 2023, p. 19

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

certain personal content sparked public discourse about freedom of expression, especially when the information pertained to personal identity and changes in one's life.

Inconsistent Implementation and Enforcement

Despite the recognition of the right to be forgotten, its implementation and enforcement remain inconsistent. Users often lack clarity regarding the data deletion process, and many encounter difficulties accessing their rights. The Kartika Putri case reflects this challenge, where, despite netizen support for the removal of her non-hijab photos, the process still relied on collective action and lacked clear procedures for handling deletion requests.

Due to the weaknesses of several concepts regulated in Law No. 19 of 2016, the Indonesian RBF regulation does not seem to support the existence of Big Data.[30] The first weakness is that the RBF concept is widely applied in Indonesia, both in terms of the type of information and the media targeted for RBF implementation. This affects the performance of Big Data technology which was originally created to manage data and information and ensure that it is available to anyone.

The principle of the right to be forgotten states that a person has the legal right to delete information relating to him/her that is accessible online and has the potential to interfere with his/her personal life, or simply to remove such information from search engine results. European Commissioner for Justice, Human Rights and Citizenship Viviane Reding stated that if a data controller later wants to delete a person's personal data, the data must be deleted from the system if there is no legal basis for storing it.[31] This discussion also compares the legal framework in Indonesia with the GDPR, which shows that although there has been progress in recognizing digital rights, Indonesia still has significant shortcomings in terms of procedural clarity and effective enforcement mechanisms. The Kartika Putri case underscores the need for a stronger legal framework to support user rights in the context of social media, where information can spread quickly and is difficult to remove.

Comparison with International Law

This situation also underscores the broarder comparison between Indonesia's legal framework with international standards, such as the GDPR. It shows thatthat while there has been progress in recognizing digital rights, Indonesia still has significant shortcomings in terms of procedural clarity and effective enforcement mechanisms. The Kartika Putri case exemplifies the need for a stronger legal framework to support user rights in the context of social media, where information can spread rapidly and be difficult to delete.

Relevance of the Kartika Putri Case

Ultimately, the Kartika Putri case serves as a concrete example of how social pressure and community support can influence an individual's decision to delete content. It demonstrates that, despite collective efforts to remove harmful content, users must still confront challenges within an unstructured deletion process. This highlights the importance of clear legal and procedural support to ensure that the right to be forgotten can be effectively implemented.

Need for Policy Reform

[30] SETYARDI, Heribertus Untung. Indonesian Legal Readiness: Regulation of Right to be Forgotten in Relation to Big Data. *Jurnal Kewarganegaraan*, 2023, 7.1: 1068-1079.

[31] Viviane Reding, The Upcoming Data Protection Reform for the European Union, 1 International Data Privacy Law, Volume 1, Issue 1, February 2011. Page. 3-5.

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

In practice, the implementation of the data deletion system in Indonesia is still difficult to implement because many statutory phrases have general meanings and there is no specific explanation regarding the intent of the phrase, for that reason it is necessary to redefine it to be more certain regarding the phrase Right to Delete Information or the right to be forgotten and Define the meaning of "irrelevant data".[32]

The need to form an agent who is responsible and functions to supervise and audit the privacy conditions of an application service provider whether it is truly in accordance with the principles of privacy protection in Indonesia.[33] And clearly regulate all Application Service Providers Require all application service providers to provide a facility for users to submit requests for the right to delete information by clearly explaining the rights and obligations of application service providers and data subjects in data privacy, especially the right to delete information and explaining what kind of data can be submitted for deletion

In conclusion, these observations points to the urgent need for policy reforms to enhance the clarity and enforcement of personal data rights and the right to be forgotten. This includes the establishment of more transparent and accountable procedures, as well as improved mechanisms for addressing data deletion requests. ithout clear legal support and transparent procedures, as illustrated by the Kartika Puitri case, users remain vulnerable to unwanted data exposure.

In light of the Kartika Putri case and the broader contrasts between the GDPR and Indonesia's PDP Law, several key policy recommendations are crucial to reinforcing the right to be forgotten and ensuring its practical enforcement

Policy Recommendations

First, governments and regulators need to establish clear and binding procedural standards for processing data deletion requests on social media platforms. This should include deadlines for responding to requests, obligations to provide adequate explanations if requests are denied, and mechanisms for appealing such decisions. The case of Kartika Putri illustrates the importance of transparency in this process, enabling individuals to feel heard and valued.

Equally important is the enhancement of platform accountability. Social media platforms should be legally obligated to comply with data deletion requests in a transparent and accountable manner. This could involve providing user-friendly interfaces for deletion requests, real-time status tracking, and automatic removal across mirrors and reposts. While community support played a role in Kartika Putri's case, the absence of formal procedures left the process fragmented and uncertain.

To support these efforts, the provision of independent oversight authorities is essential. These authorities should have the authority to investigate complaints, issue binding orders, and impose administrative sanctions on platforms that fail to comply with deletion requests. These authorities can also provide interpretative guidance in complex or ambiguous cases, as seen in the Kartika Putri case, where the decision to delete content was significantly influenced by social context.

[32] Ajiputera, Muhammad Taufik, and Heru Susetyo. "Implementation of the regulation of the right to be forgotten through a system of deleting personal data and/or electronic documents according to the perspective of positive law in Indonesia." UNES Law Review 6, no. 3 (2024): 8051-8067.

[33] DHARMAWAN, Ni Ketut Supasti; KASIH, Desak Putu Dewi; STIAWAN, Deris. Personal data protection and liability of internet service provider: a comparative approach. *International Journal of Electrical and Computer Engineering (IJECE)*, 2019, 9.4: 3175-3184.

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

Furthermore, implementation of implementation of content-origin-based deletion protocols would ensure that legal responses are proportionate and context-sensitive. Regulations should include distinct deletion protocols based on the origin of the content (e.g., self-posted content, reposted content, and third-party generated content). In the Kartika Putri case, the content in question had deep personal implications, highlighting the need for tailored legal responses.

Given the global nature of digital platforms, cross-border cooperation, such as encouraging international cooperation to address the transnational nature of data flows and platform operations, is also crucial. This includes reciprocal recognition agreements, interconnected complaint mechanisms, and global enforcement protocols for deletion to help bridge jurisdictional gaps. Such measures will assist individuals like Kartika Putri in protecting their rights on platforms operating beyond national borders.

At the same time, balancing the right to erasure with freedom of speech remains necesary. Policymakers must define clear legal criteria to reconcile the right to be forgotten with the principle of freedom of expression. This evaluation should take into account various contextual elements, including the person's involvement in public affairs, the precision and significance of the information, and its relevance as time progresses. The case of Kartika Putri illustrates how individual choices to remove content can intersect with broader societal debates about access to information..

Finally, digital literacy initiatives are crucial to empower users. Educating the public about their data rights, platform obligations, and procedural options is essential to foster a more informed and proactive online community. Toosl such as public guidance materials, online tutorials, and the integration of digital rights into educational curricula can ensure that individuals like Kartika Putri can understand and effectively exercise their rights in the digital environment.

4. Closing

This research has explored the legal intricacies associated with the right to be forgotten in relation to social media platforms in Indonesia, particularly emphasizing the obstacles encountered during its enforcement. Despite the acknowledgment of this right within the PDP Law, its implementation is still not optimal. Users frequently grapple with unclear policies and complicated procedures, which obstruct their capacity to manage their online presence effectively.

The case study of Kartika Putri exemplifies the efforts individuals make to redefine their public personas, yet they face significant challenges when attempting to eliminate undesirable content. This situation underscores a growing recognition of the necessity for individuals to exercise control over their personal data, while simultaneously exposing the shortcomings of the current legal frameworks in place.

Consequently, this research recommends the necessity for comprehensive policy reform to enhance clarity and accountability in the data deletion process. This includes the development of more transparent and responsive procedures, the establishment of independent oversight authorities, and cross-border cooperation to address issues arising from the global nature of digital platforms.

In conclusion, the right to be forgotten must transcend mere normative concept; it needs to be integrated into concrete and accessible legal practices. Without clear and effective measures, this right risks becoming symbolic and failing to provide genuine protection for individuals in an ever-evolving digital era. The required reforms will not only strengthen individual positions within the digital

ecosystem but also contribute to the safeguarding of democratic values and privacy, which are increasingly threatened by technological advancements.

References

Acquisti, Alessandro. "The economics of personal data and the economics of privacy." Economics 11 (2010): 24.

Anagnostopoulou, Despina. "The Role of the Court of Justice of the European Union on the Interpretation of Platform Operators and Business Users' Contracts." *In Quo vadis Commercial Contract? Reflections on Sustainability, Ethics and Technology in the Emerging Law and Practice of Global Commerce*, pp. 33-82. Cham: Springer International Publishing, 2023.

Brimblecombe, Fiona. "The public interest in deleted personal data? The right to be forgotten's freedom of expression exceptions examined through the lens of Article 10 Echr." *Journal of Internet Law 23, no. 10 (2020)*: 1-29.

Carnegy-Arbuthnott, Hannah Maeve. "Privacy, publicity, and the right to be forgotten." *Journal of Political Philosophy* (2023).

Feher, Katalin. "Digital identity and the online self: Footprint strategies–An exploratory and comparative research study." *Journal of information science 47, no. 2 (2021):* 192-205.

Gal, Michal S., and Oshrit Aviv. "The competitive effects of the GDPR." *Journal of Competition Law & Economics 16, no. 3 (2020):* 349-391.

Gawankar, Yash, and Srinivas Naik. "Anticipating the Evolution of Data Accountability through Technological Advancements and Regulatory Landscape Changes." I*n Cloud Security*, pp. 143-159. Chapman and Hall/CRC, 2024.

Inam Ul Mansoor, Sheikh. "An Interface between Digital Privacy and Human Rights: The Challenges Ahead." Available at *SSRN 5019128* (2023).

Liu, Chi, Tianqing Zhu, Jun Zhang, and Wanlei Zhou. "Privacy intelligence: A survey on image privacy in online social networks." *ACM Computing Surveys 55, no. 8 (2022):* 1-35.

Minaei, Mohsen, S. Chandra Mouli, Mainack Mondal, Bruno Ribeiro, and Aniket Kate. "Deceptive deletions for protecting withdrawn posts on social media platform." *In NDSS.* 2021.

Park, Tae Jung, and Akshita Rohatgi. "Balancing the platform responsibility paradox: A case for amplification regulation to mitigate the spread of harmful but legal content online." *Computer Law & Security Review 52 (2024): 105960*.

Prastyanti, Rina Arum, and Ridhima Sharma. "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India." *Journal of Human Rights, Culture and Legal System 4, no. 2 (2024)*: 354-390.

Ringel, Sharon, and Rivka Ribak. "Platformizing the past: The social media logic of archival digitization." *Social Media+ Society 10, no. 1 (2024): 20563051241228596*.

Sadovska, Diana. "THE RIGHT TO BE FORGOTTEN: ESTABLISHMENT AND DEVELOPMENT." Visnyk of the Lviv University. *Series Law 74, no. 74 (June 30, 2022):* 68–78.

Jurnal Ilmiah Penelitian
LAW_JURNAL
E-ISSN : 2746-4571
P-ISSN : 2746-3966
Volume VI, Nomor 1,
Juli, 2025

Valenzuela-García, Noelia, Diego J. Maldonado-Guzmán, Andrea García-Pérez, and Cristina Del-Real. "Too lucky to be a victim? An exploratory study of online harassment and hate messages faced by social media influencers." *European journal on criminal policy and research 29, no. 3 (2023):* 397-421.