Vol. 22 No. 2 September 2026

YURISDIKSI

Jurnal Wacana Hukum dan Sains

Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

Concept of Regulating The Mechanism For Deleting Personal Data And Deleting Indexes In Order To Ensure Legal Certainty

Anas Rafi Prakasya[1*], Patricia Audrey Ruslijanto[1], Rachmi Sulistyarini[1]

[1]Faculty of Law, Brawijaya University Malang, Indonesia

*Corresponding Author E-mail: nsrfprksy089@student.ub.ac.id

Article History: Received: March 10, 2026; Accepted: May 07, 2026

ABSTRACT

Digital transformation has accelerated the massive use of personal data in various sectors, including government, business, health, and public services. However, the increasing use of digital systems also raises risks of data breaches, misuse of information, and the persistence of harmful digital footprints. This study analyzes the legal regulation of personal data erasure and de-indexing mechanisms in Indonesia and examines the extent to which these mechanisms provide legal certainty for data subjects and data controllers. The research employs a normative juridical method using statutory, conceptual, and comparative approaches. The study finds that Indonesia has recognized the right to erasure and the right to delisting through the ITE Law, Government Regulation Number 71 of 2019, and Law Number 27 of 2022 concerning Personal Data Protection. Nevertheless, implementation remains problematic due to fragmented regulations, unclear procedural standards, limited institutional oversight, and the absence of comprehensive implementing regulations. Therefore, regulatory harmonization, the establishment of independent supervisory institutions, clear procedural mechanisms, and increased public digital literacy are essential to ensure effective personal data protection and legal certainty in Indonesia.

Keywords: Data Deletion, De-Indexing, Legal Certainty, Personal Data Protection, Privacy Rights.

1. INTRODUCTION

The development of the internet can no longer be understood simply as an advancement in communications technology, but rather as a major revolution that has completely transformed human life. The arrival of the internet in Indonesia since the mid-1990s marked the beginning of a significant social transformation, as various activities previously carried out manually and conventionally began to shift to faster, more practical, and more efficient digital systems. The internet has fostered the birth of a new space in society: cyberspace, which enables the exchange of information without geographical or time constraints. In this context, digitalization is not just about tools, but about changing the structure of modern life. Digital transformation has had a significant impact on patterns of social interaction. Communication, which previously relied heavily on face-to-face interactions, has shifted to online media such as email, instant messaging applications, social media, and video conferencing. Personal, professional, and even institutional relationships increasingly take place through digital platforms. These changes demonstrate that information technology has become a primary means of forming relationships between individuals and between communities and institutions. As a result, the personal data generated from each digital interaction is becoming increasingly substantial and increasingly valuable. (Sutedi, 2014).

YURISDIKSI
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

In the education sector, technological advances have also fundamentally transformed learning methods. Conventional classroom-centered education systems are now evolving toward online and hybrid learning. Students can access learning materials from various regions through digital platforms, while educators can deliver materials virtually and with a wider reach. The digitalization of education expands access to knowledge, but at the same time creates a new ecosystem that collects vast amounts of personal data from students, teachers, and educational institutions. In the employment sector, digitalization is driving changes in work patterns to become more flexible. The concepts of remote working, hybrid working, and platform-based work are now commonplace. Companies are using digital systems to recruit, monitor performance, store employee data, and conduct administrative transactions. This demonstrates that workers' personal data is a crucial part of the modern work system. Therefore, the protection of workers' data is becoming an increasingly relevant legal issue amid the increasing use of technology in industrial relations.

In the economic sphere, the internet has given rise to an electronic commerce system, or e-commerce, that allows transactions to be conducted without physical contact between sellers and buyers. Marketplaces and online stores make it easier for people to obtain goods and services from various locations quickly. For businesses, digital technology opens up new markets that were previously difficult to reach. However, behind these benefits lies the massive collection of consumer data, from personal identity and addresses to shopping habits and payment methods. This data has become a highly valuable economic asset. The development of the digital economy shows that personal data is now not only related to a person's identity but also has a strong commercial dimension. Digital companies utilize user data for market analysis, targeted advertising, and product development. This situation raises legal issues when data is processed without valid consent or used beyond its original purpose. Thus, personal data protection is not just a privacy issue, but also concerns economic justice and consumer protection.

In the government sector, digitalization has given rise to the concept of electronic government (e-government). Various public services, such as creating identity documents, paying taxes, applying for permits, and other administrative services, can now be accessed online. The government also uses digital platforms to gather public input and expedite bureaucratic services. This demonstrates that digital technology has become a crucial instrument in realizing effective and transparent governance. In addition to public services, the government is also utilizing digital systems for data-driven policymaking. Through the use of big data, the government can more accurately understand public needs, map social problems, and formulate more targeted policies. Data integration between agencies, such as population, health, taxation, and social security data, is

YURISDIKSI
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

a crucial foundation for modern state governance. However, the broader the integration, the greater the risk of misuse and leakage of personal data.

Conceptually, personal data is any information that can identify an individual, either directly or indirectly. This definition aligns with international standards such as the European Union's General Data Protection Regulation (GDPR). Personal data includes name, address, identity number, location, health, consumption habits, and even biometric data. Because this data is closely related to an individual's dignity and autonomy, its protection should be viewed as part of human rights. In practice, personal data management in Indonesia is not yet fully supported by an adequate protection system. Various state institutions and the private sector collect vast amounts of data, but not all of them have robust cybersecurity standards. Many electronic systems remain vulnerable to hacking, misuse of internal access, and leaks due to administrative negligence. This situation raises serious concerns about the security of public data in the digital age. (European Union, 2016). (United Nations, 1948). (Budi Suhariyanto, 2014).

These concerns are evident in the numerous major data breaches that have occurred in Indonesia. Leaks of BPJS Kesehatan participant data, PLN customers, SIM card registration data, and even passport data demonstrate weak information security governance. The leaked data often includes sensitive information such as full names, addresses, ID numbers, payment statuses, and other administrative information. These large-scale data breaches demonstrate that personal data protection is not yet optimal. The impact of data breaches goes beyond the loss of information confidentiality. In many cases, leaked data is used for fraud, illegal online loans, identity theft, and even financial abuse. Victims often experience economic loss, difficulty accessing financial services, and psychological stress due to debt collection intimidation. This demonstrates that personal data breaches have a real impact on individuals' lives, requiring a serious and effective legal response. (Sembiring, 2019).

In addition to data breaches, the digital era also presents a new challenge in the form of digital footprints that are difficult to erase. Personal information once published online can continue to appear through search engines even if it is no longer relevant or detrimental to the data owner. Old news stories, resolved cases, personal photos, and other sensitive information can remain available and easily accessible to the public. This situation raises questions about an individual's right to repair their reputation and control their digital identity. In this context, the concept of the right to be forgotten has developed, namely the right of an individual to request the deletion of certain personal data or the removal of information that is no longer relevant from search indexes. This right aims to provide individuals with the opportunity to protect their privacy and prevent ongoing harm from legacy digital footprints. However, the implementation of this

ISSN print 2086-6852 and ISSN Online 2598-5892

right must be carried out carefully to avoid conflicting with the public interest, freedom of expression, and the right to information.

Indonesia has actually recognized the normative basis for personal data protection through the Electronic Information and Transactions Law. Article 26 of the ITE Law stipulates that the use of personal data through electronic media must be with the consent of the data owner. Amendments to the ITE Law also introduce a mechanism for deleting electronic information based on a court order. This provision forms the foundation for the right to be forgotten in national law. Furthermore, strengthening personal data protection is carried out through Law Number 27 of 2022 concerning Personal Data Protection. This law recognizes the rights of data subjects, including the right to access, correct, and delete certain personal data. The introduction of the Personal Data Protection Law is a progressive step in strengthening the position of citizens as the legitimate owners of their personal data. However, issues remain regarding the synchronization of norms and mechanisms for implementing the rights to data deletion and deletion of indexes. (Harahap, 2017).

The main problem lies in the lack of clarity in operational procedures regarding how requests for personal data deletion are submitted, which institution is authorized to make decisions, what the standards for assessing public interest are, and what the obligations are for search engines and electronic system providers in implementing them. This lack of clarity creates legal uncertainty for the public, digital businesses, and law enforcement officials. Consequently, normatively recognized rights cannot necessarily be effectively implemented in practice. Based on these conditions, it is necessary to formulate a conceptual regulation of the mechanism for personal data deletion and de-indexing that can guarantee legal certainty in Indonesia. Such regulations must balance individual privacy rights with the public interest in information, press freedom, and digital accountability. With a clear, transparent, and proportional mechanism, Indonesia can realize equitable personal data governance that aligns with the principles of the rule of law in the era of digital transformation. This study offers novelty by specifically formulating the conceptual regulation of personal data erasure and de-indexing mechanisms in Indonesia from the perspective of legal certainty for both data subjects and data controllers, while also comparing Indonesia's framework with international standards such as the GDPR.

2. RESEARCH METHODS

This study employs normative juridical legal research using statutory, conceptual, and comparative approaches. The statutory approach examines relevant legal instruments, including the 1945 Constitution of the Republic of Indonesia, the ITE Law, Government Regulation Number 71 of 2019, and Law Number 27 of 2022 concerning Personal Data Protection. The conceptual approach analyzes doctrines and legal theories related to privacy rights, legal certainty, and

ISSN print 2086-6852 and ISSN Online 2598-5892

personal data protection. In addition, the comparative approach compares Indonesia's legal framework with international standards, particularly the European Union's General Data Protection Regulation (GDPR). Legal materials consist of primary, secondary, and tertiary legal materials analyzed descriptively and prescriptively to formulate legal arguments regarding the regulation of personal data erasure and de-indexing mechanisms. (Marzuki, 2021). (Ministry of State Secretariat of the Republic of Indonesia, 2019).

3. RESULTS AND DISCUSSION

Legal Regulations for Deletion of Personal Data and Deletion of Indexes in the Indonesian Legal System

1. Constitutional and Philosophical Basis for Personal Data Protection in Indonesia

Legal regulations regarding the deletion of personal data and the deletion of indexes in the Indonesian legal system cannot be separated from the constitutional basis regarding the protection of human rights. In a state based on the rule of law, every citizen has the right to a sense of security, honor, dignity, and protection of their private life. The Indonesian Constitution, through Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, affirms that every person has the right to protection of themselves, their family, honor, dignity, and property under their control. This provision forms the basis for the protection of personal data as an integral part of the protection of the personal self of citizens. In the development of digital society, personal data is no longer viewed merely as administrative information, but has become a representation of a person's identity in cyberspace. Name, address, telephone number, health history, consumption preferences, social media track record, and biometric data are elements that describe an individual's existence as a whole. Therefore, misuse of personal data is actually a form of violation of a person's privacy rights. When data is used without permission, disseminated without a legal basis, or continues to be displayed in digital space even though it is no longer relevant, it harms not only the administrative aspect, but also human dignity and honor. (Asshiddiqie, 2010). (Warren & Brandeis, 1890).

Philosophically, the right to erasure of personal data stems from the principle that every individual should have control over information about themselves. This principle is known in various modern legal systems as informational self-determination, which refers to an individual's right to determine how their personal data is collected, used, stored, and deleted. In the Indonesian context, this principle aligns with the values of Pancasila, particularly the second principle concerning just and civilized humanity, which places humans as the primary subject whose dignity must be respected. Furthermore, the regulation regarding de-indexing also has a strong philosophical basis. In the era of digital search engines, outdated information that has lost its

ISSN print 2086-6852 and ISSN Online 2598-5892

relevance can still easily appear through internet search results. This often leads to reputational damage, employment barriers, social pressure, and even discrimination. Therefore, de-indexing aims to protect an individual's reputation and future without having to completely delete information from its original source.

The state, as the executor of power, is obligated to provide legal certainty regarding these rights. Without clear regulations, the public will experience difficulties when requesting data deletion or de-indexing of detrimental information. Conversely, electronic system administrators will also face uncertainty in determining the limits of their legal liability. Therefore, legal regulations regarding the deletion of personal data and de-indexing are an urgent need within the national legal system. Thus, the constitutional and philosophical foundations of personal data protection demonstrate that the right to data deletion is not an additional, secondary right, but rather a fundamental human right that the state must guarantee. These regulations must be understood as an instrument for protecting citizens in facing the increasingly complex challenges of the digital era. (Hadjon, 1987).

2. Normative Regulations on Deletion of Personal Data and Deletion of Indexes in Indonesian Legislation

Normatively, Indonesia already has a number of legal instruments governing the protection of personal data, although these regulations have developed gradually and are scattered across various laws and regulations. In the early stages, regulations regarding personal data did not yet stand as a separate legal regime, but rather remained part of information technology and electronic transaction law. This is evident in the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions, which was the initial milestone in regulating digital activities in Indonesia. Although the main focus of this law is electronic transactions and the use of electronic systems, it contains important norms regarding the use of personal data. Article 26 paragraph (1) of the ITE Law stipulates that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. This provision shows that Indonesian law has from the outset recognized the principle of consent as the basis for the legitimacy of personal data processing. This means that a person cannot freely use another person's personal data without the permission of the data owner. This principle is very important because it positions the individual as a subject who has control over their personal data. (Ministry of State Secretariat of the Republic of Indonesia, 2008).

However, the provisions in the ITE Law at that time were still general in nature and did not specify in detail the types of personal data, the rights of data subjects, the obligations of data controllers, or the data deletion mechanism. As a result, the legal protection provided was still very limited and unable to address the complexity of rapidly evolving digital issues. In practice, many

YURISDIKSI
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

disputes related to the misuse of personal data were difficult to resolve because a comprehensive legal instrument was not yet available. A significant development occurred when Law Number 19 of 2016 was issued as an amendment to the ITE Law. Through this amendment, Article 26 was added paragraphs (3) and (4) which introduced a mechanism for deleting irrelevant electronic information. This provision states that every Electronic System Organizer is obliged to delete irrelevant electronic information and/or electronic documents at the request of the person concerned based on a court order. This norm became the basis for recognizing the concept of the right to be forgotten in the Indonesian legal system. (Harahap, 2017). (Ministry of State Secretariat of the Republic of Indonesia, 2016).

The introduction of this concept is significant because Indonesian law is beginning to recognize that individuals have the right to request the deletion of certain digital traces that are detrimental to them. In many cases, outdated information that is no longer relevant remains publicly accessible via the internet and search engines. As a result, individuals can experience reputational damage, employment barriers, social discrimination, and even psychological distress. Therefore, the right to request the deletion of irrelevant information is a crucial protection instrument. However, the provisions in the ITE Law still require a court order. On the one hand, this requirement guarantees objectivity and prevents arbitrary abuse of the right to deletion. However, on the other hand, this mechanism has the potential to burden the public by requiring a time-consuming, costly litigation process and requiring specific legal knowledge. This raises questions about the effectiveness of access to the right to data deletion, especially for the general public with limited resources. (Harahap, 2017).

Furthermore, regulatory strengthening was carried out through Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This regulation is crucial because it explicitly introduced the terms "right to erasure" and "right to delisting" into Indonesian law for the first time. The right to erasure is understood as the right of a data subject to request the removal of certain personal data from an electronic system, while the right to delisting is the right to request the removal of search engine results from specific information. (Ministry of State Secretariat of the Republic of Indonesia, 2019).

Distinguishing between these two concepts has significant legal implications. Data erasure means removing data from a data controller's storage system or database. Meanwhile, delisting doesn't necessarily remove information from the original source, but rather limits its accessibility through search engines. In other words, news or content remains on the original site, but it is no longer easily found through general searches. This approach is often used to balance individual privacy rights with press freedom and the public interest in archived information. Subsequently, Law No. 27 of 2022 concerning Personal Data Protection was enacted, marking a major milestone

YURISDIKSI
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

in Indonesia's data protection regime. This law shifts the sectoral approach toward a comprehensive one. Under the Personal Data Protection Law, data subjects are granted various rights, including the right to obtain information, the right to access data, the right to rectify data, the right to withdraw consent, the right to restrict processing, and the right to delete and destroy personal data in accordance with legal provisions. This demonstrates that the right to data erasure has now gained significantly stronger legitimacy. (Ministry of State Secretariat of the Republic of Indonesia, 2022).

The Personal Data Protection Law also stipulates the obligations of personal data controllers to maintain data security, process data lawfully, notify data protection failures, and respect the rights of data subjects. Thus, data deletion is no longer simply an individual request, but rather a part of legal compliance governance that must be implemented by both public and private organizations. However, despite the increasingly comprehensive normative framework, several issues remain. First, there are no implementing regulations that detail the procedures for requesting data deletion and de-indexing. Second, there are no clear parameters regarding the meaning of "irrelevant," "inaccurate," "outdated," or "disproportionately detrimental." Third, there are no detailed dispute resolution mechanisms if an electronic system operator rejects a data subject's request.

Furthermore, harmonization between regulations remains a challenge. The ITE Law, the PP PSTE, and the PDP Law have different terminological approaches, often leading to confusion in practice for digital businesses, law enforcement officials, and the public. Therefore, policy synchronization and the creation of implementing regulations are urgently needed to ensure the Indonesian legal system truly provides legal certainty in the exercise of the right to delete personal data and de-index. Therefore, it can be concluded that Indonesia has normatively recognized and regulated the right to delete personal data and de-index through various regulations. However, the effectiveness of this protection still depends heavily on procedural clarity, normative harmonization, and institutional readiness for implementation.

3. Challenges in Implementing and Reforming Personal Data Deletion Laws in Indonesia

Although Indonesia has a legal basis for the deletion of personal data and de-indexing, its practical implementation still faces significant challenges. The first challenge is the low level of legal and digital literacy among the public. Many citizens do not yet understand their rights as data subjects, including the right to request access, correction, restriction of processing, or deletion of personal data. As a result, when data misuse or the dissemination of harmful information occurs, the public is often unaware of the legal recourse available. This low awareness renders the rights granted by law ineffective. In many cases, the public simply accepts the situation as their personal data is disseminated online, used for unauthorized promotional purposes, or misused by certain

ISSN print 2086-6852 and ISSN Online 2598-5892

parties. However, in a modern data protection regime, individuals should have an active and empowered position in controlling information about themselves.

The second challenge is the unpreparedness of some electronic system operators to fulfill their legal obligations. Many digital companies, online platforms, and public institutions lack clear internal procedures for following up on data deletion requests. Some lack easily accessible complaint channels, lack standard response times, and lack mechanisms for verifying the applicant's identity. This results in slow, opaque, and even ignored data deletion requests. Beyond administrative readiness, technical readiness is also a crucial issue. In modern digital systems, personal data is often scattered across multiple servers, backup systems, derivative databases, and even shared with third parties. Therefore, data deletion is not simply a matter of pressing the "delete" button; it requires an information technology system designed from the outset with the principle of privacy by design. Without adequate technical infrastructure, the right to deletion will be difficult to achieve.

The third challenge relates to the conflict between privacy rights and the public interest. Not all information can be simply deleted at an individual's request. Information relating to public officials, serious crimes, journalistic interests, historical archives, scientific research, or consumer protection may still require public access. In these situations, the state must balance the individual's right to privacy with the public's right to information. Indonesia currently lacks a detailed balancing test mechanism, as recognized in the European Union's GDPR practice. This lack of parameters has the potential to create two risks simultaneously. First, deletion requests may be arbitrarily rejected even if they are properly granted. Second, requests may be granted excessively, threatening press freedom and public transparency. Therefore, guidelines for balancing interests are urgently needed. Under the GDPR, the right to erasure is accompanied by detailed procedural safeguards and balancing tests between privacy rights and freedom of expression, which may serve as an important reference for Indonesia in strengthening its legal framework.

The fourth challenge is the suboptimal institutional oversight of personal data protection. An effective data protection regime requires an independent authority with the authority to receive complaints, conduct investigations, impose administrative sanctions, issue technical guidelines, and resolve disputes. Without a strong oversight body, law enforcement will be scattered and uncoordinated, making it difficult to restore data subjects' rights quickly. Another challenge is the transboundary nature of the internet. Indonesian citizens' personal data can be processed by global companies based overseas. Search engines, social media, cloud providers, and international digital platforms often operate across jurisdictions. Under these conditions, enforcing data deletion or de-indexing orders faces jurisdictional and law enforcement challenges. Countries need to build international cooperation and strengthen the principle of extraterritoriality in data protection laws.

ISSN print 2086-6852 and ISSN Online 2598-5892

From a legal reform perspective, Indonesia needs to immediately establish detailed implementing regulations regarding the mechanisms for deleting personal data and de-indexing. These regulations should at least address application procedures, administrative requirements, processing timeframes, objection procedures, identity verification for applicants, data controller obligations, and sanctions for non-compliance. Clear procedures will provide legal certainty for the public and businesses. Furthermore, national guidelines should be developed regarding the balance between privacy and the public interest. These guidelines are crucial to ensure that courts, supervisory agencies, and electronic system administrators adhere to the same standards in assessing each deletion request. Factors assessed may include the applicant's status as a public figure, the age of the information, its accuracy, the impact on reputation, and the public's interest in knowing the information.

The government also needs to encourage increased technical capacity among electronic system administrators through compliance standards, regular audits, and data protection certification. Companies and public agencies must begin implementing systems that support effective, secure, and documented data deletion. Compliance is not merely administrative; it must be reflected in technological design and organizational governance. Furthermore, public education on personal data rights must be a national agenda. Digital literacy focused solely on technology use is insufficient. The public needs to understand that personal data has significant legal and economic value and how to protect itself in the event of a violation. Public legal awareness is a crucial factor in the success of a data protection regime. Therefore, the challenges of implementing personal data deletion in Indonesia are multidimensional, encompassing legal, technological, institutional, economic, and social aspects. Therefore, legal reform must be carried out comprehensively through regulatory harmonization, strengthening supervisory institutions, technical readiness of business actors, and increasing public awareness. If these steps are implemented, the right to personal data deletion and de-indexing will not only be a norm on paper but will become a genuine instrument for citizen protection in the digital era.

Legal Certainty in the Mechanism for Deleting Personal Data and Indexes for Data Subjects and Data Controllers

1. The Concept of Legal Certainty in the Right to Deletion of Personal Data and Deletion of Indexes

Legal certainty is one of the primary objectives of law, alongside justice and expediency. In the context of a state governed by the rule of law, legal certainty is defined as a state in which legal norms are clearly formulated, are not open to multiple interpretations, are enforceable, and provide behavioral guidelines for both the public and state administrators. Legal certainty is crucial in the area of personal data protection because the legal relationship between data subjects and data

ISSN print 2086-6852 and ISSN Online 2598-5892

controllers involves privacy rights, digital technology, and rapidly evolving economic interests. Without legal certainty, the protection of individual rights is weakened, while businesses and public institutions also face the risk of unclear obligations. In the mechanisms for deleting personal data and de-indexing, legal certainty means having clear rules regarding who has the right to submit a request, to whom the request is addressed, what grounds may be used for the request, how long the request must be processed, and how disputes are resolved in the event of a rejection. If these elements are not clearly regulated, the right to erasure will remain merely a declarative norm that is difficult to implement in practice. (Mertokusumo, 2007).

For data subjects, legal certainty provides assurance that the state recognizes an individual's right to control their personal information. In the digital age, personal data is often widely disseminated through search engines, social media, commercial applications, and electronic government systems. If an individual does not have access to deletion mechanisms, they are potentially subject to continued harm from outdated information, incorrect data, or unauthorized data dissemination. Therefore, legal certainty serves as a means of protecting privacy, reputation, and human dignity. For data controllers, legal certainty is also crucial. Data controllers need clarity regarding the limits of their obligations to store, process, correct, and delete data. Without clear guidelines, data controllers risk being sued for negligence, or conversely, excessive deletion of data, harming the public interest. Legal certainty prevents disproportionate compliance burdens and provides operational standards that can be consistently applied.

In the Indonesian legal system, the concept of legal certainty is closely related to Article 28D paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the right of every person to recognition, guarantees, protection, and fair legal certainty. This constitutional provision is the basis that personal data protection is not sufficient to be recognized as an abstract right, but must be supported by clear and accessible mechanisms for the public. Legal certainty must also be understood not only as the existence of written rules, but also the consistency of the application of the law. In many areas, regulations are in place but their implementation varies from one institution to another. In the context of deleting personal data, consistency is important because similar requests should be treated with relatively the same standards, unless there are objective reasons that differentiate them.

Furthermore, legal certainty relates to the balance of rights and obligations. Data subjects do have the right to request data deletion, but this right is not unlimited. In some circumstances, data still needs to be preserved due to legal obligations, evidentiary interests, journalistic interests, or other public interests. Therefore, legal certainty requires clear boundaries to prevent disproportionate conflicts between rights. Therefore, legal certainty in the mechanisms for deleting personal data and de-indexing is a fundamental requirement in a digital state governed by the rule

ISSN print 2086-6852 and ISSN Online 2598-5892

of law. This certainty must be present for data subjects as rights holders, and for data controllers as the parties bearing obligations. Without it, personal data protection will be in a gray area that is detrimental to all parties.

2. Legal Certainty Regulation Conditions for Data Subjects and Data Controllers in Indonesia

Currently, Indonesia has several legal bases that provide recognition of the right to delete personal data and de-index, but the level of legal certainty is still developing. Some of the main relevant regulations are Law Number 19 of 2016 concerning Amendments to the Electronic Information and Transactions Law, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Law Number 27 of 2022 concerning Personal Data Protection. The ITE Law, through Article 26 paragraph (3), provides the basis that Electronic System Operators are required to delete irrelevant electronic information at the request of the person concerned based on a court order. This provision is important because it confirms the existence of legal channels for individuals to recover their rights. However, this norm still leaves questions regarding what is meant by "irrelevant," what the procedure for submitting a request to the court, who must be sued or petitioned, and what the timeframe for implementation is. (Harahap, 2017). (Ministry of State Secretariat of the Republic of Indonesia, 2016). (Ministry of State Secretariat of the Republic of Indonesia, 2019).

From the data subject's perspective, this situation indicates that rights have been recognized, but the implementation procedures are not yet entirely simple and accessible. Individuals harmed by negative digital footprints must understand the legal process, prepare documents, and navigate formal mechanisms that are not always easy for the general public. Thus, normative legal certainty exists, but practical legal certainty remains limited. Government Regulation Number 71 of 2019 further clarified this by introducing the terms "right to erasure" and "right to delisting." The introduction of this terminology represents a positive development, as Indonesian law begins to differentiate between deleting data from a system and de-indexing it from search engines. However, this regulation does not yet provide complete technical details regarding assessment standards, response deadlines, decision formats, or objections if a request is rejected. (Ministry of State Secretariat of the Republic of Indonesia, 2019).

For data controllers, this situation creates compliance uncertainty. On the one hand, they are obligated to respect data subjects' rights. On the other hand, they lack sufficiently detailed technical guidelines to determine when a request should be granted or can be legitimately denied. As a result, data controllers are often on the defensive, making decisions based on their own internal policies rather than uniform national standards. Law Number 27 of 2022 concerning Personal Data Protection provides a more comprehensive development. This law regulates data

YURISDIKSI
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

subjects' rights to terminate processing, delete, and destroy personal data in accordance with statutory provisions. Furthermore, the Personal Data Protection Law also stipulates the obligation of data controllers to maintain security and be responsible for data processing. Normatively, this strengthens legal certainty because the data protection regime now stands as a separate legal system.

However, current legal certainty is still affected by the incompleteness of implementing regulations. Many provisions in the Data and Information Privacy Law require derivative regulations for optimal implementation, for example, regarding the procedures for deletion requests, notification forms for data subjects, identity verification standards, and administrative dispute resolution mechanisms. As long as these derivative regulations are incomplete, there is considerable room for interpretation. Current conditions also indicate that data deletion mechanisms across digital platforms operate differently. Some global companies have relatively clear deletion request forms, while some domestic businesses lack specific procedures. This disparity in practice indicates that legal certainty has not been fully standardized in digital business practices in Indonesia.

Furthermore, the suboptimal institutional framework for overseeing personal data protection also impacts legal certainty. A data protection system requires an authority that can provide guidance, receive complaints, and impose sanctions. If these functions are not fully implemented, data subjects and data controllers alike lack an authoritative point of reference. Therefore, the current regulatory environment can be said to provide a foundation for legal certainty normatively, but it does not yet fully provide operational legal certainty. Rights and obligations have been regulated, but technical mechanisms, implementation standards, and enforcement agencies still require further strengthening.

3. Problems and Directions for Strengthening Legal Certainty

The main problem with legal certainty in the current mechanism for erasing personal data and indexing is the gap between norms and implementation. The law recognizes the right to erasure, but the public still struggles to exercise this right effectively. Many data subjects are unsure where to submit requests, how to format requests, what documents are required, and how long requests should be processed. Another issue is the lack of objective parameters for reasons for erasure. In practice, individuals can request erasure because data is inaccurate, irrelevant, processed without consent, or detrimental to reputation. However, without clear indicators, data controllers can interpret these reasons differently. This situation creates room for inconsistent decisions and potentially leads to disputes.

Another problem is the conflict between privacy rights and the public interest. For example, someone might want to delete old news reports about a legal proceeding they've been

ISSN print 2086-6852 and ISSN Online 2598-5892

involved in. From a privacy perspective, the request is understandable. However, from a public interest perspective, the information may still be relevant. Without a balancing test, deletion decisions will be highly subjective and inconsistent. From the data controller's perspective, challenges to legal certainty arise in the form of sanctions and compliance burdens. Data controllers must establish request response systems, data security, approval documentation, and internal audits. Without clear standards, compliance costs increase, and small and medium-sized businesses may struggle to adapt.

To strengthen legal certainty, Indonesia needs to immediately draft detailed and applicable implementing regulations. These regulations should outline procedures for data deletion and indexing requests, response deadlines, the format of acceptance or rejection decisions, valid reasons for rejection, and an administrative appeals mechanism. This will ensure that all parties have uniform guidelines. Furthermore, the establishment and strengthening of a personal data protection supervisory authority is crucial. This authority must be independent, professional, and empowered to resolve disputes expeditiously. The existence of a supervisory body will increase public trust and provide certainty to data controllers regarding applicable compliance standards.

The government also needs to encourage the development of sectoral guidelines. For example, data deletion mechanisms in the banking sector are certainly different from those in the health, education, or digital media sectors. A sectoral approach will make regulations more realistic and tailored to the characteristics of each sector without diminishing general data protection principles. Furthermore, improving digital legal literacy must be part of national policy. Data subjects who understand their rights will be more easily able to utilize available mechanisms. Conversely, data controllers who understand their obligations will be better prepared to build a culture of compliance and good data governance.

Going forward, legal certainty will not be measured solely by the number of regulations, but also by the public's ease of access to legal protection. A good system allows individuals to submit requests simply, receive decisions within a reasonable time, and have an effective appeals channel if harmed. Therefore, legal certainty in the mechanism for deleting personal data and indexing in Indonesia is currently in a transitional stage toward a more mature system. The legal foundation is in place, but its effectiveness depends heavily on implementing regulations, strengthening oversight bodies, standardizing practices, and increasing legal awareness of all stakeholders.

4. CONCLUSION

Indonesia has recognized the right to personal data erasure and de-indexing through the ITE Law, Government Regulation Number 71 of 2019, and the Personal Data Protection Law.

ISSN print 2086-6852 and ISSN Online 2598-5892

Nevertheless, the existing regulations remain fragmented and lack comprehensive implementing mechanisms. Legal certainty for data subjects and data controllers is still limited due to unclear procedures, inconsistent standards, and weak institutional oversight. Therefore, harmonization of regulations, establishment of implementing rules, strengthening of supervisory authorities, and enhancement of digital legal literacy are necessary to ensure effective and fair personal data protection in Indonesia. (Ministry of State Secretariat of the Republic of Indonesia, 2019).

Legal certainty regarding the mechanism for deleting personal data and indexing for both data subjects and data controllers is currently still in its infancy. Normatively, the rights and obligations of the parties have been regulated, but in practice, there are still obstacles in the form of unclear application procedures, assessment parameters for reasons for deletion, completion deadlines, objection mechanisms, and the suboptimal institutional framework for monitoring personal data protection. This situation creates the potential for multiple interpretations and inconsistent implementation in the field. Therefore, regulatory harmonization, the establishment of comprehensive technical regulations, the strengthening of independent supervisory authorities, and increased digital legal literacy are needed to ensure legal certainty in personal data protection is truly realized in a fair, effective, and sustainable manner.

REFERENCES

Asshiddiqie, J. (2010). The Indonesian Constitution and Constitutionalism. Jakarta: Sinar Grafika.

Budi Suhariyanto. (2014). Information technology crimes (cybercrime): The urgency of regulation and legal loopholes. Jakarta: Rajawali Pers.

Fuady, M. (2011). Theory of the modern legal state (Rechtstaat). Bandung: Refika Aditama.

Hadjon, PM (1987). Legal protection for the people in Indonesia. Surabaya: Bina Ilmu.

Harahap, MY (2017). Discussion of problems and application of the Criminal Procedure Code. Jakarta: Sinar Grafika.

Ministry of Communication and Informatics of the Republic of Indonesia. (2016). Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. Jakarta: Kominfo. (Ministry of Communication and Informatics of the Republic of Indonesia, 2016).

Ministry of State Secretariat of the Republic of Indonesia. (2008). Law Number 11 of 2008 concerning Electronic Information and Transactions. Jakarta: State Secretariat. (Ministry of State Secretariat of the Republic of Indonesia, 2008).

Ministry of State Secretariat of the Republic of Indonesia. (2016). Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. Jakarta: State Secretariat. (Ministry of State Secretariat of the Republic of Indonesia, 2008). (Ministry of State Secretariat of the Republic of Indonesia, 2016).

YURISDIKSI
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

Ministry of State Secretariat of the Republic of Indonesia. (2019). Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Jakarta: State Secretariat. (Ministry of State Secretariat of the Republic of Indonesia, 2019).

Ministry of State Secretariat of the Republic of Indonesia. (2022). Law Number 27 of 2022 concerning Personal Data Protection. Jakarta: State Secretariat.

Kusumaatmadja, M. (2006). Legal concepts in development. Bandung: Alumni.

Marzuki, PM (2021). Legal research. Jakarta: Kencana.

Mertokusumo, S. (2007). Understanding the law: An introduction. Yogyakarta: Liberty.

Rahardjo, S. (2009). A state based on law that makes its people happy. Yogyakarta: Genta Press.

Sembiring, S. (2019). Personal data protection from a national legal perspective. Journal of Law & Development, 49(3), 580–602.

Soekanto, S., & Mamudji, S. (2015). Normative legal research: A brief review. Jakarta: Rajawali Pers.

Sutedi, A. (2014). Telematics law. Jakarta: Sinar Grafika.

United Nations. (1948). Universal Declaration of Human Rights. New York: United Nations.

European Union. (2016). General Data Protection Regulation (Regulation (EU) 2016/679). Brussels: European Parliament and Council.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.