IURIS NOTITIA: JURNAL ILMU HUKUM
Vol. 4, No. 2, October 2026, pp. 407–421
e-ISSN: 3025-4477
Open access

Limits on the Application of the Right to Be Forgotten to Criminal Records on Public Interest Grounds in Indonesia

Ayu Riska Amalia [a]*, Atika Zahra Nirmala [b], Zahratul 'Ain Taufik [c], Hafina Haula Arsy [d]

[a,b,c] Department of Law, Faculty of Law, Social Sciences, and Political Science, Universitas Mataram, Mataram, Indonesia

[d] Department of Law, Faculty of Law, Universitas Indonesia, Depok, Indonesia

*Corresponding Author: aramel@unram.ac.id

ABSTRACT

The persistence of online criminal records creates tension between privacy and rehabilitation and the competing interests of freedom of expression, press freedom, and public access to information. This study examines the substantive and procedural limits of applying the right to be forgotten (RTBF) to criminal records in Indonesia. It employs normative legal research using statutory, conceptual, case, and limited comparative approaches. Legal materials are analysed qualitatively and prescriptively through grammatical, systematic, and teleological interpretation, supported by a proportionality test. The findings reveal that Indonesia's legal framework, comprising the Electronic Information and Transactions Law, Government Regulation No. 71 of 2019, and the Personal Data Protection Law, lacks comprehensive criteria for determining when criminal records become irrelevant or when public interest justifies their continued accessibility. This regulatory gap risks inconsistent decisions and insufficient consideration of affected parties. The study argues that RTBF is not an absolute entitlement to erase historical information but requires contextual assessment of accuracy, legal status, offence seriousness, elapsed time, rehabilitation, the data subject's public or professional role, victims' interests, risks to vulnerable groups, and journalistic, scientific, and historical value. Its principal contribution is a graduated remedial framework prioritising correction, updating, anonymisation, access restriction, and de-indexing before source deletion. The study further proposes procedurally fair judicial proceedings that enable affected parties to participate and require transparent proportionality reasoning. These proposals provide normative guidance for reconciling privacy protection and social reintegration with freedom of expression and legitimate public interest in Indonesia's digital environment.

Keywords: Right to Be Forgotten, Criminal Records, Public Interest, Privacy, Proportionality.

Article History: Received: August 5, 2026 | Accepted: October 20, 2026 | Published: October 31, 2026

How to Cite:

Amalia, A. R., Nirmala, A. Z., Taufik, Z. A., & Arsy, H. H. (2026). Limits on the Application of the Right to Be Forgotten to Criminal Records on Public Interest Grounds in Indonesia. *Iuris Notitia: Jurnal Ilmu Hukum*, 4(2), 407–421. DOI: https://doi.org/10.69916/iuris.v4i2.627

1. INTRODUCTION

The development of the internet allows personal information to be accessed, copied, and distributed quickly and easily across geographical and temporal boundaries. Such information may remain available for a long time even when it no longer reflects the person's current circumstances. This benefits access to information but also creates risks to a person's privacy, honour, reputation, and social life. Individuals therefore need adequate control over the use and dissemination of personal information about them.

The right to privacy is a human right recognised in various instruments, both in international law, such as Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (United Nations Human Rights Committee, 1988), and in the Indonesian legal system. This protection is reflected in Article 28G(1) of the 1945 Constitution of the Republic of Indonesia (Indonesia, 1945) and Article 29(1) of Law No. 39 of 1999 on Human Rights (Indonesia, 1999a). Indonesia also ratified the International Covenant on Civil and Political Rights through Law No. 12 of 2005.

In the digital environment, privacy protection has developed into a need to give individuals authority over personal data and information available on the internet. One form of this protection is the right to be forgotten

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

(RTBF). In general, this right allows a person to request the erasure of, or the termination of access to, personal data and information that are no longer relevant, inaccurate, excessive, unlawfully obtained, or no longer necessary for the purposes of processing. This right matters because a person's digital footprint can continue to affect their life, including access to employment, education, housing, financial services, and opportunities to participate in society again.

In Indonesia, recognition of the right to be forgotten was first introduced through the amendment to the Electronic Information and Transactions Law in Article 26(3) of Law No. 19 of 2016 (UU ITE) (Indonesia, 2008). This provision requires Electronic System Operators (PSE) to erase irrelevant electronic information and/or electronic documents under their control at the request of the person concerned, based on a court order. Further provisions are set out in Government Regulation No. 71 of 2019 (Indonesia, 2019).

Protection of this right was subsequently strengthened through Law No. 27 of 2022 on Personal Data Protection (UU PDP) (Indonesia, 2022). This law gives personal data subjects the right to terminate the processing of, erase, and/or destroy personal data about them. Personal data controllers are also required to erase data when they are no longer necessary to achieve the purposes of processing, consent has been withdrawn, the data subject has made a request, or the data were obtained or processed unlawfully. Nevertheless, the Personal Data Protection Law focuses more on the erasure of personal data, whereas UU ITE covers the broader categories of electronic information and documents.

These provisions leave several normative issues unresolved. One of the main issues is the lack of clear limits on what constitutes 'irrelevant information'. Applying RTBF requires a contextual assessment. Information considered no longer relevant to the data subject may remain relevant to society. This uncertainty can create a conflict between an individual's right to privacy and the public's right to information. Without clear parameters, RTBF could be used to erase information that still has historical, journalistic, or public interest value.

The issue becomes more complex when an erasure request concerns criminal records. The Personal Data Protection Law (Indonesia, 2022) classifies criminal records as specific personal data. On the one hand, the continued availability of criminal records on the internet can create digital stigma that follows a person after their sentence has ended and can hinder rehabilitation and social reintegration. The continued availability of criminal records on the internet can hinder rehabilitation and social reintegration. On the other hand, society may have a legitimate interest in knowing about certain criminal histories, particularly where they concern the safety of vulnerable groups, sexual offences, human rights violations, corruption, fraud, professional malpractice, or the records of public officials.

The right to be forgotten therefore cannot be applied without limits. Each erasure request must be assessed according to the nature of the information, the time since publication, the data subject's position and role, the degree of public interest, the impact of dissemination on the individual, and the risks that may arise if the information is erased. A case-by-case approach and the application of proportionality are needed to achieve a fair balance between the right to privacy, freedom of expression, freedom of the press, and the public's right to information.

Another issue concerns the mechanism for enforcing this right. The erasure of irrelevant electronic information under UU ITE requires a court order. A voluntair application procedure is essentially directed towards the applicant's interests alone. Yet the erasure of information may affect the interests of Electronic System Operators, the media, data controllers, and society. If these parties have no opportunity to explain why the information should be retained, the proceedings may fail to consider all relevant matters. This shows the need for a mechanism that ensures a fair legal process while allowing the court to assess all affected interests.

The Personal Data Protection Law does provide exceptions to the exercise of data subjects' rights, including for national defence and security, law enforcement, state administration, financial sector supervision, and statistical and scientific research purposes (Indonesia, 2022). However, these exceptions do not expressly cover the exercise of freedom of expression and freedom of information. This differs from the approach in the European Union's General Data Protection Regulation (GDPR) (Regulation , EU), which explicitly treats freedom of expression and information as a limit on the exercise of the right to be forgotten.

This account shows that the development of the right to be forgotten in Indonesia has advanced privacy and personal data protection but leaves uncertainty about its scope, the criteria for information that may be

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

erased, public interest exceptions, and the procedures for resolving requests. Further study is therefore needed to establish the limits on applying the right to be forgotten, particularly to criminal records, so that it does not become a means of removing information important to society. Its regulation and application must effectively protect privacy and individuals' opportunities for rehabilitation without sacrificing freedom of expression, the public's right to know, legal certainty, and the public interest.

Studies of the right to be forgotten in Indonesia generally focus on the recognition of erasure rights in UU ITE and UU PDP or compare them with Article 17 of the GDPR (Regulation , EU). These discussions do not always distinguish between data erasure by controllers, deletion of information at its original source, and de-indexing by search engines. Nor are sufficiently operational parameters available to determine when criminal records still carry a public interest and which remedy is most proportionate. This analytical gap matters because choosing between retaining information and deleting it entirely may sacrifice privacy and rehabilitation on one side, or freedom of the press, victims' interests, public safety, and historical value on the other.

In response to these issues, this study proceeds from the argument that the right to be forgotten in relation to criminal records is not an absolute right to erase history, but a right to a contextual assessment of continued processing and ease of digital access. This assessment must apply a proportionality test (Cohen-Eliya & Porat, 2011; Stone Sweet & Mathews, 2008) that considers the accuracy and legal status of the information, the seriousness of the offence, the time elapsed, rehabilitation, the subject's position, the relationship between the information and public functions or professions based on trust, victims' interests and safety, risks to vulnerable groups, and journalistic, scientific, and historical value.

Unlike an approach that treats this issue as a binary choice between retaining and deleting information, this study proposes a graduated model of remedies. Correction, updating, anonymisation, access restriction, and de-indexing must be considered before source deletion. This study also proposes proceedings that allow data subjects, PSE, the media or publishers, victims, and other interested parties to be heard before the court determines the remedy. The study thus contributes public interest parameters, a sequence of remedies, and a design for proceedings that can be used in applying Indonesian law.

2. RESEARCH METHOD

This is a normative legal study using statutory, conceptual, case, and comparative approaches (Hutchinson & Duncan, 2012; Marzuki, 2017). The statutory approach examines the 1945 Constitution of the Republic of Indonesia, UU ITE, the Personal Data Protection Law, Government Regulation No. 71 of 2019, and other regulations relating to privacy, public information, and criminal records. The conceptual approach examines the right to be forgotten, the right to privacy, rehabilitation, public interest, freedom of expression, and proportionality. The case approach examines the reasoning in relevant cases and practices, including *Google Spain*, while the comparative approach is applied in a limited manner to the GDPR and developments in European law to inform an assessment of Indonesian law, rather than to transfer foreign provisions directly. Primary legal materials comprise legislation, human rights instruments, and relevant court judgments. Secondary legal materials include books, journal articles, institutional reports, and policy documents.

These materials were collected through library research and then analysed qualitatively and prescriptively using grammatical, systematic, and teleological interpretation. To determine the limits on applying the right to be forgotten, this study uses a proportionality test comprising a clear legal basis; a legitimate aim for the restriction; the suitability of the measure for that aim; necessity or the absence of less restrictive alternatives; and a balance between the harm to the data subject and the public benefit of retaining the information.

3. RESULT AND DISCUSSION

3.1. The Right to Be Forgotten in Indonesian National Law

a. The Basis of the Right to Privacy and the Development of RTBF in Indonesia

Every individual has the right to control and decide the extent to which their personal information may be shared with the outside world. This concept is known as the 'right to privacy' (Solove, 2007). The right to privacy involves an individual's right to control their personal information and decide whether, how, and with whom it may be shared. In data protection, this control relates, among other things, to knowledge of data collection, access to personal data, restrictions on the purposes of data use, and, in certain circumstances,

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

consent to the use or disclosure of data to others.

Privacy as a human right requiring protection is recognised in Article 12 of the 1948 Universal Declaration of Human Rights (United Nations General Assembly, 1948) and further affirmed in Article 17 of the 1966 International Covenant on Civil and Political Rights (United Nations Human Rights Committee, 1988). Both instruments prohibit arbitrary or unlawful interference with privacy and guarantee legal protection against attacks on a person's honour and reputation. In Indonesia, the right to privacy is reflected in Article 28G(1) of the 1945 Constitution (Indonesia, 1945), which guarantees the right to protection of a person's personal data. Article 29(1) of Law No. 39 of 1999 on Human Rights (Indonesia, 1999a) also states that 'everyone has the right to protection of their person, family, honour, dignity, and property', alongside Law No. 12 of 2005 ratifying the international covenant, the ICCPR.

On the basis of these legal instruments, several laws in different sectors subsequently set out requirements to protect individual rights and personal data. Guarantees for the protection of citizens' personal data are set out in a number of statutory provisions. With the emergence of the digital era and the widespread dissemination of information through the internet, the need for privacy protection in the digital world has increased. This prompted the emergence of a new concept of a right that gives individuals authority to erase their personal information from the internet, known as the right to be forgotten.

In general, the right to be forgotten allows individuals, in certain circumstances, to request the erasure of personal data concerning them (the right to erasure) or to limit how easily the information can be found by removing certain links from search results based on a person's name (de-indexing or delisting). The concept developed significantly through the judgment in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, before the Court of Justice of the European Union (CJEU) (Court of Justice of the European Union, 2014), and was subsequently codified in Article 17 of the General Data Protection Regulation (GDPR) (Regulation , EU).

A similar development can be found in Indonesian law. RTBF first acquired an explicit legal basis through the 2016 amendment to UU ITE (Indonesia, 2008) and was then detailed in Government Regulation No. 71 of 2019 (Indonesia, 2019). Its provisions must subsequently be read together with Law No. 27 of 2022 on Personal Data Protection (Indonesia, 2022), particularly the provisions on Personal Data Subjects' rights and the duties to erase and destroy Personal Data. The development of RTBF in Indonesia therefore does not stand alone but forms part of the broader development of privacy and personal data protection in the digital environment.

b. Right to Be Forgotten dalam Kerangka Hukum Indonesia

In Indonesian law, provisions on the right to be forgotten are spread across UU ITE, Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions, and the Personal Data Protection Law. The objects, subjects, and mechanisms of these three instruments are not entirely the same. Applying RTBF must therefore begin by determining the type of information concerned, the party controlling or processing it, and the measure requested.

Article 26(3) of Law No. 19 of 2016 amending the Electronic Information and Transactions Law requires PSE to erase irrelevant Electronic Information and/or Electronic Documents under their control at the request of the person concerned, based on a court order (Indonesia, 2008). In this context, PSE include parties that provide, manage, and/or operate electronic systems. Electronic Information and Electronic Documents must be understood according to their definitions in UU ITE. The PSE, the type of information, its storage location, and the requested measure must be identified before the court determines whether the application is justified.

Government Regulation No. 71 of 2019 (Indonesia, 2019) then clarifies that this mechanism may take the form of information erasure (the right to erasure) or removal from search engine listings (the right to delisting). This distinction matters because the two measures have different legal consequences.

This article therefore conceptually distinguishes three measures that are often conflated: data erasure by data controllers, deletion of information at its original source, and de-indexing or delisting by search engines. The three measures differ in the intensity of their restrictions and their consequences. Determining a remedy must therefore be preceded by identifying the controller, the location of the information, the purposes of processing, and the affected parties.

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

c. Irrelevant information that May be Erased

UU ITE protects privacy by giving individuals the right to request the erasure of personal information about them that is no longer relevant. The exercise of this right involves the court in assessing the legal basis and merits of an erasure application. This provision on 'irrelevant information' is conceptually consistent with the right to be forgotten as developed in the CJEU's judgment in *Google Spain* (Court of Justice of the European Union, 2014). The judgment is an important comparative reference because it shows that the relevance of information may change over time. Data initially processed lawfully and accurately may become irrelevant or unnecessary if their processing continues beyond the original purposes of collection. The judgment's reasoning helps explain the meaning of 'irrelevant information' in UU ITE, although its application must still be adapted to the Indonesian legal system.

Closer examination, however, shows that the protection provided by UU ITE still has normative weaknesses that may cause problems in its application. One such weakness is the absence of clear limits and indicators for the meaning of 'irrelevant information'. This uncertainty leaves broad scope for interpretation, particularly when an individual's interest in personal data protection conflicts with the public's interest in obtaining and accessing information.

Without strict criteria and a transparent assessment mechanism, the right to be forgotten could be misused to erase or restrict public access to a person's record. An erasure application, for example, may target information about a person's involvement or alleged involvement in past human rights violations, corruption, or other serious crimes. Applying the right to be forgotten must therefore consider more than the applicant's privacy interests: it must also take into account the nature of the violation, the applicant's position in public life, the historical value of the information, victims' interests, and the public's right to information.

The CJEU's judgment does not establish a fixed standard for when information may be considered irrelevant or no longer relevant, or for how much time must pass before a person may request erasure (Court of Justice of the European Union, 2014). The relevance of information is therefore not determined solely by the time since its publication. The CJEU places the determination of relevance within an assessment of the circumstances of each case. This assessment must consider the nature and sensitivity of the information, the time elapsed, the purposes of processing, the individual's position in public life, and the public's interest in continued access to the information. A case-by-case approach is needed to achieve a proportionate balance between privacy and personal data protection, freedom of expression, and the public's right to information. Uncertainty about the limits of relevance therefore does not automatically confer broad authority to erase information, but requires contextual scrutiny and the application of proportionality to each request.

The national legal framework does not specifically define 'irrelevant information'. However, Article 16(1) of Government Regulation No. 71 of 2019 (Indonesia, 2019) provides several criteria for Electronic Information and/or Electronic Documents whose erasure may be requested through the right to erasure mechanism. These criteria cover Personal Data obtained and processed without the owner's consent; data for which processing consent has been withdrawn; data obtained or processed unlawfully; data no longer consistent with the purposes for which they were obtained; data used beyond the specified period; and/or data displayed by an Electronic System Operator in a manner that harms the Personal Data owner.

Although it provides operational criteria, the provision does not fully explain how to assess the relevance of information, particularly when an erasure application conflicts with the public interest. This issue becomes more complicated when the information requested for erasure concerns criminal records, a person's position in public life, or an event of historical value. Article 16(2) also states that the duty to erase does not apply to information that must be retained or whose erasure is prohibited by legislation. The criteria in Article 16 therefore cannot be applied automatically but must be assessed in light of the context, the public interest, and the legal duty to retain the information. Government Regulation No. 71 of 2019, Article 16.

The foregoing means that irrelevant information is not necessarily incorrect information. Information that was initially true, lawful, and relevant may lose its relevance when the purposes of processing have been achieved, the retention period has ended, or changed circumstances mean that its dissemination is no longer proportionate to its original purpose. Relevance may therefore relate to time, context, accuracy, and the impact on the data subject. Nevertheless, these criteria do not fully establish a standard for assessing the relevance of information when an erasure application conflicts with the public interest, particularly in relation to criminal records.

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

Law No. 27 of 2022 on Personal Data Protection also does not clearly define 'irrelevant information', particularly when the erasure of personal data conflicts with the public interest (Indonesia, 2022). Article 16(2) of UU PDP requires data collection to be limited, specific, lawful, and transparent; processing to accord with its purposes; and data to be processed accurately, completely, without being misleading, in an up-to-date manner, and accountably. The provision also requires personal data to be erased or destroyed after the retention period ends or at the data subject's request, unless otherwise provided by legislation. These principles indicate that data no longer related to the purposes of processing, no longer current, or retained beyond their retention period may substantively be regarded as having lost their relevance. However, the provision does not provide adequate parameters for determining whether information should still be retained because it carries a public interest, including information on criminal records.

Article 8 of UU PDP also gives data subjects the right to terminate the processing of, erase, and/or destroy personal data about them. Accordingly, personal data controllers must terminate processing when the retention period has been reached, the purposes of processing have been fulfilled, or the data subject has made a request. Erasure is required when the data are no longer necessary to achieve the purposes of processing, consent has been withdrawn, the data subject has made a request, or the data were obtained or processed unlawfully. When the retention period ends or the data subject makes a request, the data must be destroyed. This approach uses a functional parameter: the relevance of data is determined by the relationship between the data and the purposes of processing, rather than solely by the data owner's subjective assessment.

Compared with UU ITE, which uses the term 'irrelevant Electronic Information and/or Electronic Documents', UU PDP focuses specifically on personal data. This difference in the subject matter creates a problem when an application targets not only particular data but also news reports, archives, or documents that contain personal data and have public value.

d. Right to Be Forgotten terhadap Rekam Jejak Kejahatan

The purpose of the right to be forgotten is to protect individuals from the effects of processing and disseminating personal data that no longer have a lawful basis or purpose (Mayer-Schönberger, 2009). In relation to criminal records, this situation means that the information may remain available even after legal proceedings have concluded and the person has served their sentence. Nevertheless, the fact that information constitutes personal data does not, by itself, entitle the data subject to erase it. Criminal records may also have journalistic, historical, and public interest value that justifies continued access. Applying the right therefore requires clear identification of the types of personal data that may be erased after meeting these criteria.

Article 4(2) of UU PDP (Indonesia, 2022) classifies criminal records as specific personal data. Criminal records are written records of a person who has committed an unlawful act or is undergoing judicial proceedings, including police records and inclusion on lists preventing departure or entry. The classification of criminal records as specific personal data indicates that their processing may create greater risks to the data subject's rights and interests and therefore requires a higher level of protection.

Criminal records must, however, be distinguished from all information about crime that can be found on the internet. Police records, investigation data, court judgments, state institution archives, media reports, and public comments have different sources, purposes, and legal consequences. Similarly, information about alleged offences, designation as a suspect, trial proceedings, acquittals, discharges from all legal charges, and convictions that have become final and binding cannot be treated as the same category. The subject matter of an application must therefore be established before assessing whether erasure is justified. Erasure from a controller's database, deletion of a news report at its original source, anonymisation of archives, and removal of links from search engine results differ in the degree of restriction and their legal consequences.

Protection of criminal records is closely related to the aims of rehabilitation and social reintegration (Stacey, 2017). A person who has served their sentence should, in principle, have the opportunity to participate in society again. The continued availability of criminal records may create stigma and hinder access to employment, education, housing, financial services, and social relationships (Lageson, 2022). Search engines may also bring up old events solely on the basis of a person's name, so that those events create a picture that no longer fully reflects their identity and current life. In certain circumstances, the ease of finding old information may extend the effects of punishment beyond the sanction imposed by the court.

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

Looking back, these considerations have a historical connection with the concept of *droit à l'oubli*, or the right to oblivion: the idea that a person who has served their sentence should not continually face publications about past wrongdoing (de Terwangne, 2012). In the digital environment, this idea has developed into a demand to reassess continued processing and ease of access to personal data. This development does not mean that historical facts must be erased or that an offence for which the sentence has been served never occurred. The issue is whether a person's identity still needs to be readily linked to that event indefinitely.

The public's interest in information does not automatically disappear because of the interest in rehabilitation. Criminal records may contribute to public safety, the protection of vulnerable groups, scrutiny of power, assessment of public officials' integrity, and accountability in professions based on trust. These interests may carry substantial weight, for example in cases involving sexual offences against children, serious violence, corruption, gross human rights violations, fraud in professional relationships, or conduct indicating an ongoing risk. In such circumstances, deleting information entirely may reduce the public's ability to protect itself and scrutinise those exercising power or public responsibility.

For citizens in general, information about a person's criminal record is an expression of the right to information and provides early protection against potential crime they may encounter, making it a matter of public interest. Nevertheless, public interest must not be equated with public curiosity. Information carries a public interest when access to it provides a tangible benefit for safety, accountability, scrutiny of power, protection of vulnerable groups, or understanding of events of social and historical value. A subject's popularity or intense public attention to an event does not, by itself, justify retaining and disseminating personal information indefinitely. Conversely, a person's status as an ordinary citizen does not automatically eliminate the public interest if their criminal history remains connected to ongoing activities, professions, or risks.

This approach can be seen in developments in European law. In *Google Spain*, the CJEU recognised that the processing of data initially lawful and accurate may become inappropriate over time if the data are no longer adequate, irrelevant or no longer relevant, or excessive in relation to the purposes of processing (Court of Justice of the European Union, 2014). However, the removal of links from search results must still consider the public's interest in information, particularly when the subject has a role in public life. The judgment concerns the removal of links from search results based on a person's name, rather than deletion of information at its original source. *Google Spain* is therefore used as a comparative reference for understanding changes in the relevance of information and the need to balance rights, rather than as a provision directly binding in Indonesia.

A more specific approach to criminal records is found in *Hurbain v. Belgium* (European Court of Human Rights, 2023). The case concerned an old article about a fatal road traffic accident that remained available in a media outlet's digital archives. The European Court of Human Rights accepted the anonymisation of the offender's name after considering the time elapsed, the offender's rehabilitation, their status as an ordinary citizen, the impact of digital access on their reputation, and the preservation of the original archive's integrity. The judgment shows that a remedy need not always involve deleting all the information. Anonymisation can protect the data subject without removing an archive's journalistic and historical value.

As in Europe, the right to erase personal data concerning a person's criminal history or records in Indonesia must therefore be limited by balancing privacy rights and the public interest. In some criminal cases, the public has an interest in knowing about the offence so that people who interact with the offender can protect themselves. The treatment of criminal records as a matter of public interest can be seen in countries such as the United States, where criminal records, like most criminal proceedings, are generally considered public (Lageson et al., 2021).

Under Indonesian law, data subjects' rights to terminate processing and request the erasure and/or destruction of personal data may include criminal records because those records are classified as specific personal data (Indonesia, 2022). However, UU PDP does not provide that every criminal record may be erased merely at the data subject's request. The right under Article 8 is limited by other provisions, including exceptions for law enforcement proceedings, the public interest in state administration, and statistical and scientific research purposes under Article 15. Article 44 also recognises that data still connected to the resolution of legal proceedings cannot simply be destroyed.

Nevertheless, the national legal framework does not yet provide complete parameters for assessing requests to erase criminal records. UU PDP focuses on the basis and purposes of data processing, while UU ITE uses

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

the concept of irrelevant electronic information and/or electronic documents. Neither expressly determines how the time elapsed, rehabilitation, the data subject's position, the seriousness of the offence, victims' safety, journalistic value, historical interest, and the public's right to know should be considered together. This gap creates a risk of inconsistent application: justified requests to protect rehabilitation may be rejected, while requests intended to conceal information important to the public may be granted.

The right to be forgotten in relation to criminal records should therefore not be understood as a right to erase historical facts or make an event appear never to have occurred. It is better understood as a right to a contextual assessment of whether the processing of, and ease of digital access to, criminal records still serve a legitimate purpose proportionate to their impact on the data subject. The outcome need not be a binary choice between retaining and deleting information. Under the principles of necessity and proportionality, remedies may be graduated through updating, correction, anonymisation, access restriction, or de-indexing. Deletion at the original source should be a last resort when less restrictive measures are inadequate and the information no longer has public value that can justify its continued dissemination.

e. Exception to The Right to be Forgotten

The right to be forgotten needs to be governed by clear principles and balanced against other interests, particularly freedom of expression, the public's right to information, law enforcement, state administration, and archiving, research, and historical documentation. In addition to determining whether information contains personal data, the application of RTBF must assess whether continued processing and access still have a lawful basis and are necessary and proportionate. The main criterion is therefore a 'fair balance' between the legitimate public interest in information and the data subject's right to data protection.

This balancing approach is expressly set out in Article 17(3) of the General Data Protection Regulation (GDPR) (Regulation , EU). Under this provision, the right to erasure does not apply insofar as processing remains necessary for exercising freedom of expression and information; complying with a legal obligation or performing a task in the public interest or in the exercise of official authority; the public interest in health; archiving in the public interest, scientific or historical research, and statistical purposes; or establishing, exercising, or defending legal claims. These criteria relate directly to the assessment of the public interest, freedom of expression, the data subject's position, the nature of the information, and the context of processing.

These exceptions show that erasure cannot be ordered merely because information harms a person's reputation or is no longer wanted by the data subject. It must be examined whether the information remains necessary to protect other interests also recognised by law. In news reporting, Article 85 of the GDPR requires Member States to reconcile personal data protection with freedom of expression and information, including processing for journalistic, academic, artistic, and literary purposes (Regulation , EU). The GDPR's protection framework therefore does not treat privacy and freedom of information as a binary choice; the two must be reconciled through an assessment of necessity and proportionality.

In Indonesian law, restrictions on data subjects' rights are found in Article 15 of Law No. 27 of 2022 on Personal Data Protection (Indonesia, 2022). This provision excludes the exercise of certain rights, including the right to terminate the processing of, erase, and/or destroy personal data under Article 8.

These exceptions include:

- national defence and security;
- law enforcement proceeding;
- the public interest in state administration;
- supervision of the financial services sector, monetary matters, payment systems, and financial system stability; and
- statistic and scientific research.

UU PDP (Indonesia, 2022) explains that the interests of law enforcement proceedings include efforts to implement or enforce legislation, including preliminary investigation, investigation, and prosecution. The public interest in state administration includes population administration, social security, taxation, customs, and

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

electronic business licensing services. UU PDP also states that these exceptions may only be applied in implementing statutory provisions. Exceptions therefore cannot be used arbitrarily but must have a legal basis, a legitimate purpose, and a clear connection to the interest to be protected. UU PDP itself classifies criminal records as one category of specific personal data.

Articles 15 and 43 of UU PDP must be read systematically. Article 43 requires controllers to erase personal data when the data are no longer necessary to achieve the purposes of processing, consent has been withdrawn, the data subject has made a request, or the data were obtained or processed unlawfully. Article 15, meanwhile, limits the exercise of certain data subjects' rights where specific interests protected by law are involved. Article 15 is therefore not a general exception to all data processing principles, but a restriction on the exercise of particular rights in specified circumstances.

Although it provides restrictions, the structure of UU PDP does not yet offer fully adequate parameters for balancing the right to erasure with freedom of expression and the public's right to information. Unlike Article 17(3)(a) of the GDPR, Article 15 of UU PDP does not explicitly cite the exercise of freedom of expression and information as a ground for an exception to the right to erasure. Journalistic interests, historical documentation, and the preservation of public archives are also not set out in detail as grounds for assessing erasure requests. Scientific research interests are mentioned, but the provision does not provide criteria for distinguishing retention genuinely necessary for research from excessive processing. This gap reinforces the need for public interest parameters and a proportionality test capable of assessing each application in its context.

3.2. Public interest parameter and Proportionality test for Criminal records

Public interest cannot be equated with public curiosity. Information carries a public interest when access to it makes a tangible contribution to public safety, scrutiny of the exercise of power, prevention of harm, professional accountability, protection of vulnerable groups, or understanding of events of historical and social value. A subject's popularity or intense public attention therefore does not, by itself, justify retaining and disseminating criminal records indefinitely.

a. The accuracy and Legal Status of the Information

Determining the limits of the right to be forgotten must begin by ensuring that the information is accurate, lawfully obtained, and related to legal proceedings whose status is clear. Information about allegations, designation as a suspect, trial proceedings, judgments that are not yet final and binding, acquittals, discharges from all legal charges, and final and binding convictions carries different weight and reputational consequences. Information that is inaccurate, misleading, incomplete, or not updated to reflect the final outcome of legal proceedings must therefore first be corrected. In such circumstances, correction or updating may be more appropriate than complete deletion.

In *TU and RE v. Google LLC*, the CJEU stated that search engine operators must de-index information if the applicant can show that the contested information is manifestly inaccurate (Court of Justice of the European Union, 2022). However, the applicant does not first have to obtain a court judgment against the information's publisher to prove that inaccuracy.

Where the problem concerns incomplete information, a proportionate remedy may therefore include adding the final status of the case, publishing a right of reply, correcting the headline, linking to the latest judgment, or explaining that the person has been acquitted. Deletion becomes relevant only if the inaccuracy cannot be corrected or the processing lacked a lawful basis from the outset.

b. Public Interest

Once the accuracy and legal status of the information have been established, the public interest must be assessed on the basis of several interrelated factors. The nature and seriousness of the offence (2) the time elapse since the offence and completion of the sentence; (3) the subject's age at the time of the offence; (4) evidence of rehabilitation, reintegration, and the risk of reoffending; (5) the subject's position as a public official, candidate for public office, professional, or ordinary citizen; (6) the relationship between the past offence and the public function or work currently performed; (7) concrete risks to public safety or vulnerable groups; (8) victims' interests and safety; (9) journalistic, scientific, or historical value; (10) how the information was obtained and published; and (11) the degree of actual and continuing harm to the data subject. No single factor automatically

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

determines the outcome; all factors must be assessed in the circumstances of the particular case. The type of offence is relevant but must not be the sole basis. Sexual offences against children, corruption, gross human rights violations, serious violence, fraud involving professional trust, and offences indicating an ongoing risk generally carry greater public interest weight. However, continued access must still have a rational connection to the purpose of public protection. Conversely, minor offences committed long ago, committed when the offender was a child, followed by demonstrable rehabilitation, and no longer connected to the subject's social role may provide stronger grounds for restricting access to the information.

c. Applying the Proportionality test

Once the competing interests have been identified, a proportionality test is used to determine whether continued access or its restriction is justified (Cohen-Eliya & Porat, 2011). First, a restriction on privacy or access to information must have a legal basis whose application is foreseeable. Second, the measure must pursue a legitimate aim, such as privacy protection, rehabilitation, public safety, or freedom of information. Third, it must be suitable and genuinely contribute to that aim. Fourth, the alternative that restricts rights the least must be chosen. Fifth, the benefits of the measure must be balanced against the harm it causes to other rights. Applying these stages prevents courts from merely asserting an abstract public interest without explaining its nature, weight, and relevance.

d. Graduated Remedies

When choosing a remedy, a distinction must be made between deleting information at its original source, erasing data held by a data controller, and de-indexing or removing certain links from search results based on a person's name. Source deletion is the most intensive measure because it can remove information from media archives or lawful records. De-indexing, meanwhile, limits how easily information can be found without deleting its source. Under the principle of necessity, courts should prioritise correction, anonymisation, access restriction, or de-indexing if these measures adequately protect the data subject. Source deletion is justified only if the information is unlawful, inaccurate and cannot be corrected, or no longer serves a legitimate purpose proportionate to the harm it causes.

1. Correction or updating is used when information is inaccurate, incomplete, or does not reflect the latest developments in the case.
2. Anonymisation removes or conceals the subject's identity without deleting the substance of the event. In *Hurbain v. Belgium*, the ECtHR considered anonymisation of an online archive less restrictive of freedom of the press than deleting the entire article (European Court of Human Rights, 2023). The original version remained in the print archives, so historical integrity was not entirely lost.
3. Access restriction retains the information but limits who can access it or the purposes for which it may be used.
4. De-indexing removes certain links from search results based on the data subject's name. The information at its original source remains available and can still be found through searches based on topics, events, or other keywords.
5. Source deletion is the most intensive measure because it can remove information from media archives or lawful records. It should be used as a last resort, particularly when information was obtained or processed unlawfully, is proven inaccurate and cannot be corrected, or no longer serves a legitimate purpose proportionate to the harm it causes.

e. The Relationship between UU ITE with UU PDP

The relationship between UU ITE and the Personal Data Protection Law must also be read systematically. UU ITE governs irrelevant electronic information and/or documents and requires a court order, while the Personal Data Protection Law focuses on data subjects' rights and controllers' duties throughout the personal data processing cycle. They should not be understood as mutually exclusive regimes. When an application concerns personal data in an electronic system, the Personal Data Protection Law's principles of lawful, limited, transparent, accurate, and purpose-consistent processing may be used to interpret the element of 'irrelevance'

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

in UU ITE. At the same time, the protection of freedom of expression, the press, and access to information must remain part of the constitutional assessment.

Under these parameters, an application should not be granted if the information remains accurate, is directly related to the exercise of public office or a profession based on trust, is necessary to protect vulnerable groups, or has substantial journalistic and historical value. Conversely, an application is more justified when the information has lost its current relevance, the subject is not a public figure, the sentence was completed long ago, rehabilitation has been demonstrated, the risk to society is low, and continued access causes harm that is no longer proportionate. Between these two situations, the court may order graduated remedies through updating, anonymisation, access restriction, or de-indexing.

3.3. Mechanism for Enforcing Right to Be Forgotten in Indonesia

The mechanisms for enforcing the right to be forgotten in Indonesia are formed through the relationship between UU ITE, Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions, and the Personal Data Protection Law (Indonesia, 2008, 2019, 2022). The subject matter, grounds, and routes for erasure under these three instruments are not entirely the same. Their enforcement mechanisms must therefore be distinguished according to the type of information, the remedy requested, and the legal basis of the application.

a. Erasure and De-indexing

Electronic System Operators (PSE) are required to provide a mechanism for erasing irrelevant electronic information. First, erasure from a system under the PSE's control, or the right to erasure. Second, removal of links from search engine listings, or the right to delisting. This distinction matters because the two measures have different subject matter, procedures, and legal consequences.

Erasure from a system may remove electronic information or documents from a source controlled by a PSE. By contrast, the right to delisting, or de-indexing, does not delete information from the source website but removes its display or blocks access to certain links in search results. Thus, the information at its original source remains available and technically still be found through other search method.

Under Government Regulation No. 71 of 2019, removal from search engine listings is carried out on the basis of a court order (Indonesia, 2019). PSE are also required to provide a mechanism for erasing irrelevant electronic information. At a minimum, this mechanism includes a communication channel with personal data owners, an erasure feature, and the recording of erasure requests. The duty to provide a mechanism does not mean that every request must be granted automatically. PSE must still examine the applicant's identity, the subject matter of the request, its legal basis, the criteria for irrelevance, any retention duties, and possible legitimate interests of others or legal duties requiring the information to be retained.

PSE are, therefore, not required to accept every erasure request. A request may be rejected if the conditions for erasure are not met, the information must still be retained under a legal duty, or another interest lawfully justifies continued processing.

b. The applicant standing and Court Proceedings

An application for removal from search engine listings is submitted by the person concerned or a party authorised to act on their behalf. The application must identify the applicant, the relevant PSE, the information or documents for which restriction is sought, and the reasons why the information is considered irrelevant.

The term 'court order' indicates that the mechanism proceeds through an application rather than an ordinary civil lawsuit (voluntair jurisdiction), in which the case is brought in the form of an application submitted by the applicant, followed by a court order that the PSE must comply with if the application is granted. This voluntair action involves only one party, namely the plaintiff or applicant bringing the case, and the matter raised primarily concerns that party's interests alone. The matter is for the benefit of one party only, in that the issue raised by the applicant does not affect the rights and interests of others, and the proceedings are one-sided (ex parte).

The application is non-contentious or concerns the rights and interests of other parties. This means that the PSE is considered to have no interest in retaining the data and must therefore comply with the court order

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

without appealing. On this basis, the mechanism for erasing data through a court judgment is not difficult to reconcile with fairness, because the application for an order is a voluntair or one-party action, whereas erasure affects two parties at once: the personal data owner and the data controller (PSE).

In this situation, a PSE, as an entity or individual holding electronic information and/or electronic documents considered irrelevant, may lose control over its rights and interests in retaining and controlling that information and/or those documents. However, the PSE has no opportunity to submit objections, rebuttals, or explanations to defend its rights and interests in the information because of the voluntair nature of the action.

Nevertheless, describing the mechanism as an application does not mean that the case always concerns only one party's interests. Erasure or de-indexing may affect the rights and interests of PSE, media publishers, authors, victims, information users, and society.

The mechanism should therefore not be understood as a simple voluntair matter that has no bearing on others' rights. In right to be forgotten cases, there is in fact a conflict between the data subject's privacy and rehabilitation on one side and freedom of expression, archive integrity, and public access to information on the other.

The normative problem with Indonesia's right to be forgotten mechanism lies not merely in the use of an application procedure but in the lack of detailed procedures ensuring the participation of parties whose legal interests may be affected by the court order. Government Regulation No. 71 of 2019 requires an application for the right to delisting to include the PSE's identity and/or the electronic system's address, but does not explicitly require the PSE to be summoned or given an opportunity to provide information. This situation must be examined critically under the principle of *audi et alteram partem* (Handayani, 2020), which requires a balanced opportunity for parties whose legal interests are affected to be heard before the court issues a judgment or order. Even in civil procedural practice, a case formally submitted as an application is not always suitable for ex parte examination if its substance affects another party's legal interests.

Participation becomes even more important when the information requested for erasure carries a public interest. In certain circumstances, PSE, publishers, or the media may have a legal basis, a legitimate interest, or a duty to retain the information. UU PDP itself recognises the principles of public interest and balance, as well as legitimate interests as a basis for data processing. In news reporting, this also concerns the public's right to information and the press's role in upholding the rule of law and human rights and scrutinising the public interest. Judges therefore need to hear from affected parties so that the assessment of relevance is based not only on the applicant's interests but also on privacy, the public interest, freedom of expression, and the right to information.

c. Guarantees of a fair process

Right to be forgotten proceedings must comply with the principle of a fair process. At a minimum, the mechanism must ensure: a. notification to the PSE and the information's publisher; b. an opportunity to submit responses and evidence; c. victims' participation when their interests are affected; d. examination of the information's accuracy and legal status; e. assessment of the public interest; f. a distinction between source deletion and de-indexing; g. consideration of less restrictive alternatives; h. reasons for the judgment showing the application of a proportionality test; and i. an effective correction or legal remedy mechanism for injured parties. PSE participation is not merely intended to defend a 'right to control data'. For search engines, the media, digital libraries, or archive managers, the interests at stake may include editorial freedom, archive integrity, compliance with legal duties, and users' right to information.

UU PDP gives individuals the right to terminate the processing of, erase, and/or destroy personal data about them, and requires personal data controllers to erase Personal Data that are no longer necessary to achieve the purposes of Personal Data processing, for which the Personal Data Subject has withdrawn processing consent, whose erasure the Personal Data Subject has requested, or that were obtained and/or processed unlawfully (Indonesia, 2022).

d. Weaknesses in the National Mechanism

The national mechanism for applying RTBF still leaves various issues unresolved.

First, there are no detailed substantive parameters for assessing 'irrelevant information', particularly in

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

relation to criminal records.

Second, the procedural relationship between the right to erasure under the Personal Data Protection Law and the court order mechanism under UU ITE has not been adequately established. Third, there are no specific procedural rules expressly governing summonses, evidence, affected parties' participation, the burden of proof, and legal remedies.

Fourth, there is insufficiently clear guidance for distinguishing source deletion, anonymisation, access restriction, correction, and de-indexing.

Fifth, freedom of the press, the value of archives, victims' interests, and the public's right to know have not been explicitly made mandatory considerations in every application.

Sixth, enforcement of an order may encounter issues of jurisdiction and effectiveness if the search engine or PSE operates across national borders.

Given these weaknesses, the court mechanism cannot merely establish whether the applicant satisfies formal requirements. The court must substantively examine the information's accuracy and current relevance, the public interest, the consequences for victims, the data subject's position, and the most proportionate remedy.

The mechanism for enforcing the right to be forgotten in Indonesia should therefore be developed as a measured adversarial process, even when formally initiated through an application. Parties whose interests are affected must have an opportunity to be heard. Under this arrangement, a court order does more than give the data subject control: it also serves as a mechanism for balancing privacy, rehabilitation, freedom of expression, victims' interests, and the public's right to information.

4. CONCLUSION

The right to be forgotten in relation to criminal records cannot be understood as an absolute right to erase history. Accurate, lawfully processed information may lose its relevance because of changes in time, purpose, context, or its impact on the data subject, but erasure must still be weighed against the public interest. The assessment must consider the information's legal status, the seriousness of the offence, the time elapsed, the subject's age at the time of the act, evidence of rehabilitation and the risk of reoffending, a public position or profession based on trust, the interests of victims and vulnerable groups, and journalistic, scientific, and historical value.

UU ITE, Government Regulation No. 71 of 2019, and the Personal Data Protection Law form complementary regimes but do not yet provide adequate substantive and procedural parameters. Since erasure and de-indexing may affect PSE, the media, publishers, victims, and society, an application should not be examined solely as a matter of one party's interests. Proceedings must allow affected parties to be heard, examine the information's accuracy and current relevance, and explain the application of the proportionality test in the court's reasoning.

Policymakers need to establish guidelines distinguishing correction, updating, anonymisation, access restriction, de-indexing, erasure by controllers, and source deletion. Courts should apply graduated remedies and choose the measure that restricts rights the least: correction or updating when information is incomplete, anonymisation or de-indexing when ease of discovery is no longer proportionate, and source deletion only as a last resort when processing is unlawful, information is inaccurate and cannot be corrected, or it no longer serves a legitimate purpose proportionate to the harm it causes.

DECLARATION

Funding
The authors received no financial support of any kind for the conduct of the research, the drafting, and/or the publication of this article.

Conflicts of Interest
The authors declare no financial conflicts of interest or personal relationships that could influence, or appear to influence, the analysis results and legal arguments presented in this article.

Availability of Data and Legal Materials
All legal materials, court rulings, or supporting data analyzed in this research are fully included in this

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

manuscript.

AI Use Statement
ChatGPT was used to assist with formatting, preparing the abstract, and improving readability.

REFERENCES

Andrez Belategi, M. (2024). The right to be forgotten concerning the criminal past: Developments in the case law of the European Court of Human Rights with particular reference to the anonymisation of digital press archives. *Oñati Socio-Legal Series*, 14(6), 1639–1669. https://doi.org/10.35295/osls.iisl.1938

Bunn, A. (2015). The curious case of the right to be forgotten. *Computer Law & Security Review*, 31(3), 336–350. https://doi.org/10.1016/j.clsr.2015.03.006

Carnegy-Arbuthnott, H.M. (2023). Privacy, publicity, and the right to be forgotten. *Journal of Political Philosophy*, 31(4), 494–516. https://doi.org/10.1111/jopp.12308

Cohen-Eliya, M., & Porat, I. (2011). Proportionality and the culture of justification. *American Journal of Comparative Law*, 59(2), 463–490. https://doi.org/10.5131/AJCL.2010.0018

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.

Court of Justice of the European Union. (2019). *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, ECLI:EU:C:2019:772.

Court of Justice of the European Union. (2022). *TU and RE v. Google LLC*, Case C-460/20, ECLI:EU:C:2022:962.

de Terwangne, C. (2012). Internet privacy and the right to be forgotten/right to oblivion. *Revista de Internet, Derecho y Política*, 13, 31–43.

Erdos, D. (2021). The right to be forgotten beyond the EU: An analysis of wider G20 regulatory action and potential next steps. *Journal of Media Law*, 13(1), 1–35. https://doi.org/10.1080/17577632.2021.1884947

Erdos, D., & Garstka, K. (2020). The right to be forgotten online within G20 statutory data protection frameworks. *International Data Privacy Law*, 10(4), 294–313. https://doi.org/10.1093/idpl/ipaa012

European Court of Human Rights. (2012). *Axel Springer AG v. Germany [GC]*, Application No. 39954/08.

European Court of Human Rights. (2018). *M.L. and W.W. v. Germany*, Applications Nos. 60798/10 and 65599/10.

European Court of Human Rights. (2023). *Hurbain v. Belgium [GC]*, Application No. 57292/16.

European Data Protection Board. (2020). *Guidelines 5/2019 on the criteria of the right to be forgotten in the search engines cases under the GDPR (Part 1) (Version 2.0).*

Faisal, K. (2021). Balancing between right to be forgotten and right to freedom of expression in spent criminal convictions. *Security and Privacy*, 4(4), e157. https://doi.org/10.1002/spy2.157

Frantziou, E. (2014). Further developments in the right to be forgotten: The European Court of Justice's judgment in Case C-131/12, Google Spain. *Human Rights Law Review*, 14(4), 761–777. https://doi.org/10.1093/hrlr/ngu033

Handayani, D. (2020). Kajian filosofis prinsip audi et alteram partem dalam perkara perdata. *Jurnal Ilmiah Kebijakan Hukum*, 14(2), 385–402. https://doi.org/10.30641/kebijakan.2020.V14.385-402

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review*, 17(1), 83–119.

Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.*

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.

Indonesia. (1999). *Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia*.

Indonesia. (1999). *Undang-Undang Nomor 40 Tahun 1999 tentang Pers*.

Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024*.

Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Koops, B.-J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice. *SCRIPTed*, 8(3), 229–256.

Lageson, S. E. (2022). Criminal record stigma and surveillance in the digital age. *Annual Review of Criminology*, 5, 67–90. https://doi.org/10.1146/annurev-criminol-030920-092833

Lageson, S. E., & Maruna, S. (2018). Digital degradation: Stigma management in the internet age. *Punishment & Society*, 20(1), 113–133. https://doi.org/10.1177/1462474517737050

Lageson, S. E., Webster, E., & Sandoval, J. R. (2021). Digitizing and disclosing personal data: The proliferation of state criminal records on the internet. *Law & Social Inquiry*, 46(3), 635–665.

Marzuki, P. M. (2017). *Penelitian hukum* (Edisi revisi). Kencana.

Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.

Nuradanta, E., & Nelson, F. M. (2022). Penerapan asas audi et alteram partem dalam perkara permohonan pemberian izin poligami. *Syntax Literate: Jurnal Ilmiah Indonesia*, 7(6), 8481–8490. https://doi.org/10.36418/syntax-literate.v7i6.8034

OECD. (2002). *OECD guidelines on the protection of privacy and transborder flows of personal data*. OECD Publishing. https://doi.org/10.1787/9789264196391-en

Ramadaani, K. F., & Muaalifin, M. D. A. (2023). Analisis yuridis pengaturan hak untuk dilupakan (right to be forgotten) dalam Undang-Undang Nomor 19 Tahun 2016. *Legacy: Jurnal Hukum dan Perundang-Undangan*, 3(1), 18–41. https://doi.org/10.21274/legacy.2023.3.1.18-41

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). (2016).

Rosadi, S. D. (2018). Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal*, 5(1), 143–157. https://doi.org/10.21776/ub.blj.2018.005.01.09

Sartor, G. (2016). The right to be forgotten: Balancing interests in the flux of time. *International Journal of Law and Information Technology*, 24(1), 72–98. https://doi.org/10.1093/ijlit/eav017

Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the internet*. Yale University Press.

Stacey, C. (2017). Rehabilitation in the internet age: The Google-effect and the disclosure of criminal records. *Probation Journal*, 64(3), 269–275. https://doi.org/10.1177/0264550517711280

Stone Sweet, A., & Mathews, J. (2008). Proportionality balancing and global constitutionalism. *Columbia Journal of Transnational Law*, 47(1), 72–164.

United Nations General Assembly. (1948). *Universal Declaration of Human Rights*.

United Nations Human Rights Committee. (1988). *General Comment No. 16: Article 17 (Right to privacy)*.

United Nations Human Rights Committee. (2007). *General Comment No. 32: Article 14: Right to equality before courts and tribunals and to a fair trial (CCPR/C/GC/32)*.

United Nations Human Rights Committee. (2011). *General Comment No. 34: Article 19: Freedoms of opinion and expression (CCPR/C/GC/34)*.

Copyright © 2026 by Authors. Distributed under CC BY 4.0 International License.