

## IBLAM LAW REVIEW

P-ISSN

2775-4146

E-ISSN

2775-3174

Volume 3, Nomor 3, 2023

### Authors

Adinda Setyaning Putri

### Affiliation

Brawijaya University

### Email

Adindasetyaningputri01@gmail.com

### Date Submission

28 July 2023

### Date Accepted

01 August 2023

### Date Published

14 September 2023

### DOI

10.52249

## COMPARISON OF RIGHT TO BE FORGOTTEN (RTBF) BETWEEN INDONESIA AND SEVERAL COUNTRIES TO ESTABLISHING CERTAIN LEGAL DATA PROTECTION IN INDONESIA

### Abstract

*Right to be Forgotten (RTBF) is a legal concept representing an individual's right to control their personal data held by an electronic system operator. The legal basis for implementing the RTBF in Indonesia is outlined in Article 26 (3) and Article 26 (4) of the ITE Law, which were adopted through the first international regulation recognizing RTBF, namely Article 17 of the General Data Protection Regulation 2016. However, the implementation of RTBF in Indonesia remains a subject of debate. One of the reasons is that the ITE Law only obliges electronic system operators to provide mechanisms for deleting irrelevant information or electronic documents but does not impose sanctions on those who refuse to accept requests for data removal. This results in legal ambiguity within the ITE Law, particularly in Article 26 (3) and Article 26 (4), which form the basis for implementing the RTBF concept in Indonesia. This article aims to conduct a comparative legal approach to the implementation of RTBF in Indonesia and several other countries where RTBF has already been applied. The goal is to identify adoption models that can be considered for implementation in Indonesia to address the regulatory uncertainties surrounding RTBF implementation. The research yields several key points of discussion, including: (1) The limits of RTBF usage in Indonesia; and (2) A comparison of RTBF in Indonesia with other countries that have also implemented RTBF as a means of protecting personal data.*

**Keywords:** *Comparative Law, Legal Protection, Right To Be Forgotten.*

### Abstrak

*Right to be Forgotten (RTBF) merupakan sebuah konsep hukum berupa hak individu, dimana seseorang dapat mengendalikan data pribadi mereka yang terdapat pada sebuah penyelenggara sistem elektronik. Dasar hukum pelaksanaan RTBF di Indonesia sendiri terdapat pada Pasal 26 Ayat (3) dan Pasal 26 Ayat (4) UU ITE, yang diadopsi melalui regulasi internasional pertama yang mengakui RTBF, yakni Pasal 17 *General Data Protection Regulation* 2016. Namun, dalam pelaksanaannya, penggunaan RTBF di Indonesia masih menjadi salah satu perdebatan, dimana salah satunya yakni UU ITE hanya mewajibkan penyelenggara sistem elektronik untuk*

menyediakan mekanisme penghapusan informasi atau dokumen elektronik yang sudah tidak relevan, namun pada saat yang sama juga tidak menyediakan sanksi terhadap penyelenggara sistem elektronik yang menolak untuk menerima pengajuan penghapusan informasi atau dokumen elektronik, sehingga hal ini pada akhirnya menyebabkan adanya sebuah kekebaburan hukum dalam UU ITE, utamanya dalam Pasal 26 Ayat (3) dan Pasal 26 Ayat (4) yang menjadi dasar pelaksanaan konsep RTBF di Indonesia. Artikel ini akan berfokus untuk melakukan pendekatan komparatif hukum pelaksanaan RTBF di Indonesia dan beberapa negara lainnya yang juga sudah menerapkan RTBF di negara mereka, sehingga nantinya dapat ditemukan model adopsi yang bisa dipertimbangkan untuk diterapkan di Indonesia dalam upaya menghilangkan kekebaburan dari regulasi pelaksanaan RTBF di Indonesia. Penelitian ini menghasilkan beberapa pokok bahasan, antara lain: (1) Batas penggunaan RTBF di Indonesia; dan (2) Komparasi RTBF Indonesia dengan beberapa negara lainnya yang juga sudah menerapkan RTBF di negara mereka sebagai salah satu wujud mewujudkan perlindungan terhadap data pribadi.

**Kata Kunci:** Hak Untuk Dilupakan, Komparasi Hukum, Perlindungan Hukum.

## INTRODUCTION

We have entered an era where almost every aspect of our lives coexists with the role of technology. The presence of technology in human life undoubtedly provides many conveniences in daily life. One of these conveniences is the ability to access information about other people simply by searching for specific data related to them in an electronic system operator, such as Google. This is often done to find out someone's background or life history, and it is a common practice for HR departments in companies before recruiting new employees.

However, in daily practices, it is evident that there is a significant amount of information, both in the form of data and electronic documents within an electronic system operator, that has become irrelevant after time passes by. In response to this issue, a legal concept called the Right to be Forgotten (RTBF) emerged (Christianto, 2020). It allows an individual to request an Electronic System Operator such as Google, to remove information or electronic documents that are deemed no longer relevant to them. RTBF was adopted from a jurisprudential model in European countries in 2014 and was officially regulated in 2016 through the General Data Protection Regulation 2016. In Indonesia, the RTBF concept was introduced in 2016 through Law No. 19 of 2016 (commonly known as the ITE Law), specifically in Article 26 Paragraph (3) and Paragraph (4) of the ITE Law. However, the inclusion of the RTBF concept in the ITE Law seemed to be rushed and forced, considering that RTBF was not part of the academic study in the preparation of the draft bill to amend the ITE Law, which initially only focused on limited issues such as (1) Defamation (Article 27 Paragraph (3)); (2) Interception of communication (Article 31); (3) Procedural Law (Article 43);

and (4) Criminal Threats (Article 45). This unpreparedness is also due to the fact that Indonesia does not yet have a strong data protection and privacy regime, which can lead to conflicts such as the opinion that RTBF contradicts the right to freedom of expression; cleansing criminal records by offenders; and other similar concerns.

From the explanations above, it can be concluded that the implementation of the Right to be Forgotten (RTBF) in Article 26 Paragraph (3) and Paragraph (4) of the ITE Law as an effort to provide legal protection for irrelevant personal data cannot be considered perfect due to the legal ambiguity in its regulatory implementation. Therefore, this article will focus on making a legal comparison of the implementation of RTBF in Indonesia with several other countries, with the hope of finding an RTBF application model that can solve the legal uncertainties surrounding its implementation in Indonesia.

## **METHODS RESEARCH**

This paper employs a normative research method with a comparative, conceptual and statutory approach, which is commonly known as a research method based on concepts. The legal materials were obtained through a literature review technique, and the analysis of these materials was conducted using a prescriptive research approach. These methods are used to determine the legal boundaries of RTBF usage in Indonesia and to find an RTBF model that can be utilized to eliminate legal uncertainties surrounding the implementation of RTBF in the ITE Law.

## **RESULTS AND DISCUSSION**

### **Limitations of the Right to be Forgotten in Indonesia**

This section will explain the types of information and electronic documents that can be controlled using RTBF. Until today, Indonesia, particularly under the Information and Electronic Transactions Law (UU ITE), has not explicitly regulated or officially recognized the Right to be Forgotten (RTBF) concept as it was implemented by the European Union through the General Data Protection Regulation 2016 (GDPR). Consequently, the Indonesian Information and Electronic Transactions Law does not contain specific provisions for the RTBF (Adhari, 2021). Nevertheless, within the context of content removal or blocking under the Information and Electronic Transactions Law, there are certain scenarios where individuals can request the removal of content that involves privacy violations, defamation, or the dissemination of harmful information (Sukmawati, 2020). Some instances of cybercrimes where the Right to be Forgotten can be employed as a consideration include the following:

#### **1. Spreading harmful private information**

In cases where content or media shares someone's private information, including phone numbers, addresses, or other sensitive data, without their consent, individuals who experience material or non-material losses have the right to request the removal of such content under the provisions of the Information and Electronic Transactions Law. This law prohibits the dissemination of harmful personal electronic information. This corresponds with Article 26, paragraph (1) of the Information and Electronic Transactions Law (UU ITE), which expressly forbids individuals from intentionally disseminating electronic information that causes harm to others without proper authorization.

#### **2. Defamation**

If an individual experiences defamation through media, which includes insults, slander, or attacks on their reputation, they have the option to seek the removal of content that violates their rights through the existing legal procedures outlined in the Information and Electronic Transactions Law. Defamation is specifically addressed in Article 27, paragraph (3) of the Information and Electronic Transactions Law, which prohibits the intentional dissemination of electronic information and/or electronic documents containing defamatory statements or character attacks without proper authorization.

### 3. Copyright Violation

If an individual identifies content that violates their copyright, they have the right to request the removal of such content in accordance with the regulations outlined in the Information and Electronic Transactions Law, which specifically addresses copyright matters. Copyright infringement is governed by Article 113 of the Information and Electronic Transactions Law, which deals with criminal offenses related to copyright infringement conducted through information technology.

Also, The types of personal data that can be requested for removal based on the Right to be Forgotten (RTBF) can also be seen in Article 4 of Law No. 27 of 2022 concerning the Protection of Personal Data (PDP), which divides personal data into two categories: specific personal data and general personal data. According to Article 4 Paragraph (2) of the PDP Law, legally protected specific personal data includes health data and information; biometric data; genetic data; criminal records; data of children; personal financial data; and other data in accordance with the provisions of the legislation. On the other hand, according to Article 4 Paragraph (3) of the PDP Law, legally protected general personal data includes name; gender; nationality; religion; marital status; and personal data combined to identify an individual. There are also some legal considerations and limitations that can be outlined before applying RTBF in Indonesia (Kusna, 2019), such as:

#### 1. Privacy Safeguarding

Safeguarding privacy is of utmost importance when implementing RTBF in cases involving Deepfake Pornography. It is essential to strike a balance between individual privacy rights and public interests, freedom of expression, and access to information.

#### 2. Achieving a Balance in Freedom of Expression

RTBF must not be employed to unfairly or excessively curtail freedom of expression. It is important to find a middle ground that respects both an individual's right to be forgotten and the right to freedom of expression, taking into account any relevant public interests.

#### 3. Determination of Responsible Entities

Recognizing the entities accountable is a crucial aspect that should not be disregarded. This involves assessing whether platform providers or individuals responsible for creating and sharing such deepfake content bear the responsibility for removing or blocking unlawfully infringing information

#### 4. Criteria for Removal

Thoughtful evaluation is necessary to establish the guidelines for removing a data. Factors like content authenticity, the extent of harm caused, relevance of the information, and public interest should be thoroughly examined to determine the eligibility for deletion.

#### 5. Boundaries of Jurisdiction

RTBF might face constraints due to variations in jurisdictional laws across countries. It is essential to take into account the jurisdiction in which electronic system providers operate and

the laws governing privacy protection and content removal in that specific jurisdiction. This is also in accordance with Article 62 paragraph (1) of the PDP Law. International collaboration becomes essential in tackling these cases, emphasizing the significance of legal contemplation on procedures and mechanisms for international cooperation in the removal or blocking of illicitly infringing deepfake content.

### **Right to be Forgotten Concept Comparison**

The RTBF concept originated in the European Union in 2014, following its use by Mario Costeja Gonzales in a legal battle against Google Spain. The trial occurred from May 27, 2012, to May 13, 2014 (D Maietta, 2020). Two years later, in 2016, RTBF was formally regulated through Article 17 of the General Data Protection Regulation (GDPR) and automatically adopted by EU member states. In Indonesia, a similar concept to RTBF is present in Article 26 of the ITE Law, specifically in paragraphs three and four, resembling Article 17 of the GDPR 2016. Subsequently, this article will delve into the legal approaches of other countries that have embraced the RTBF concept as a fundamental aspect of data protection within their jurisdictions. These countries include:

#### 1. Belgium

Besides adopting the GDPR 2016, Belgium has incorporated the Right to be Forgotten (RTBF) into their legal framework through two additional regulations: the Belgian Data Protection Act 2018 and the Belgian Data Protection Executive Regulation 2019. The Belgian Data Protection Act 2018 serves as the national implementation of the GDPR 2016, outlining comprehensive provisions for safeguarding personal data in Belgium, which includes individual rights like RTBF (Escouflaire, 2023). Conversely, the Belgian Data Protection Executive Regulation 2019 offers technical and practical guidelines to support the implementation of personal data protection within the country, including specific instructions on submitting RTBF requests and the responsibilities of service providers or platforms. Moreover, Belgium has clearly defined procedures for handling RTBF requests as stipulated in Article 21 of the Belgian Data Protection Executive Regulation 2019. Additionally, Belgium is equipped with a Data Protection Authority (Belgian DPA), serving as the supervisory body responsible for overseeing and enforcing personal data protection regulations in the country.

We can see an example of the use of RTBF in Belgium through the Decision of the Belgian Human Rights Court No. 417/15, which was issued on December 13, 2022. The decision pertains to a news report involving a couple named Mr. and Ms. V, which was broadcasted on Radio Television Belge de la Communauté Française. The report featured sex videotapes belonging to the couple, which was considered a violation of their privacy rights contrary to Article 10 of the European Convention on Human Rights (ECHR). As a result, Mr. and Ms. V decided to request the application of RTBF against Radio Television Belge de la Communauté Française to the Human Rights Court. The court accepted their request and ordered Radio Television Belge de la Communauté Française to immediately remove the report involving Mr. and Ms. V through the Decision of the Belgian Human Rights Court No. 417/15 on December 13, 2022.

#### 2. France

Aside from adhering to the GDPR 2016, France has its own domestic regulations concerning RTBF, which serve to safeguard personal data. The Loi Informatique et Libertés 2018 establishes the legal foundation for implementing RTBF in France (Rey, 2022). The

specific procedures for RTBF implementation in the country are outlined in Article 9 of the Loi Informatique et Libertés 2018. Additionally, France has the Commission Nationale de l'Informatique et des Libertés (CNIL), which functions as the local enforcement authority responsible for addressing cases related to Deepfake Pornography.

An example of RTBF usage in France can be found in the Decision of the Conseil d'État (Council of State, France) with case number C-507/17, which involves a RTBF request filed by CNIL against Google France. CNIL, represented by Kent Walker, filed an RTBF request with the court concerning the alleged publication of Kent Walker's opinions uploaded by Google without permission through LeMonde Newspaper. The Conseil d'État accepted the request and imposed sanctions on Google France to promptly remove the opinions from the system. Additionally, Google France was fined \$112,000 as per the Decision of the Conseil d'État (Council of State, France) in case number C-507/17 on September 24, 2019.

### 3. Britain

Following the UK's decision to exit the European Union, they subsequently implemented the Data Protection Act 2018 (Janclute, 2020). This legislation governs the safeguarding of personal data in the UK, offering protection against the misuse of individuals' personal information. The provisions related to RTBF are outlined in Article 170 of the Data Protection Act 2018, which also provides details on the implementation of RTBF within the country. This article prohibits the intentional acquisition of personal data without valid permission.

Moreover, in the UK, if an individual's RTBF request is not addressed by a particular electronic system provider, the victim can report the case to the competent authority, namely the Information Commissioner's Office (ICO). ICO will offer legal assistance and further advice pro bono to handle the reported cases (Wachter, 2019). ICO has a dedicated web portal for submitting RTBF requests, also known as the 'Right to Erasure' there. The victim only needs to fulfill the necessary requirements and conditions set by ICO to investigate the related content, so that it can be determined whether the content can be removed or not.

One of the cases involving the use of RTBF in the United Kingdom is the Decision of the NT1 & NT2 Court against Google LLC, with case number EWCH 799 (QB) 2018. Both NT1 and NT2 submitted RTBF requests regarding information about themselves that was no longer relevant but still accessible through the Electronic System Provider (ESP), Google. NT1 had been charged with fraud in the late 1990s, while NT2 had received a 6-month sentence for attempted interception of communications. This contradicted Article 8 of the Data Protection Directive regarding Sensitive Data. Therefore, the court accepted the RTBF requests from NT1 & NT2 and ruled that Google LLC must promptly remove the information about the old cases involving NT1 & NT2 from their electronic systems.

### 4. South Korea

South Korea is one of the countries in East Asia that highly values the privacy of individuals' personal information. In practice, if someone wishes to request the deletion or restriction of personal information, they can directly contact the responsible party of the platform or website. Regarding RTBF in South Korea, it is regulated in South Korea under the Personal Information Protection Act (PIPA) of 2011 (Craft, 2019). PIPA safeguards personal information and grants individuals the right to delete or restrict the use of their personal information if it is unauthorized or in violation of the law. This is explained in Article 30 of

PIPA 2011, where an individual can request the removal of their personal data if it has been used unlawfully.

However, as we know, direct requests to the platform responsible for the electronic system are rarely responded to (Mahmud, 2020). In such cases, if this happens, the victim can report the incident to the Korea Communications Standards Commission, abbreviated as KCC. KCC has its own website for reporting crimes related to the misuse of personal information, accessible through [privacy.go.kr](http://privacy.go.kr). The victim only needs to provide the necessary information requested by KCC to further investigate the case, which will determine whether the related information can be removed or not. If the perpetrator is found to have misused the victim's personal data, the sanctions that can be imposed on the perpetrator according to Article 65 of the Personal Information Protection Act (PIPA) of 2011 are a maximum prison sentence of 5 years and a fine of up to 50 million won.

When we compare with Indonesia, it is apparent that Indonesia is relatively lagging in terms of RTBF, which is stated in Article 26 paragraph (3) and Article 26 paragraph (4) of the Information and Electronic Transactions Law (UU ITE). Currently, Indonesia does not have specific legal regulations concerning the implementation of RTBF, RTBF procedures, or sanctions against electronic system providers who violate these provisions. In Indonesia, there is still no clear procedure for individuals to utilize RTBF in cases of personal information misuse affecting them. Although Indonesia has enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP), this law also refers to Article 17 paragraph (1) of the GDPR 2016 and does not include specific limitations on RTBF usage in Indonesia, as stated in Article 17 paragraph (3) of the GDPR 2016, which is limited to areas such as health, archival activities related to public interests, research, and statistics. The absence of limitations on RTBF usage in Indonesia can lead to potential conflicts with other legislations in Indonesia, such as Law Number 40 of 1999 concerning the Press (Jamaludin, 2020).

Furthermore, there is no specialized officer or authority in Indonesia responsible for handling cases of personal information misuse beyond the police. Consequently, many reports are not effectively addressed since the Indonesian police are authorized to deal with various types of criminal cases, leading to arguments that Indonesia should establish a separate authority outside the police to handle cyber cases, including the misuse of personal information, for more effective resolution (Rahmadani, 2023). Pasurama, a Program Officer at the Institute for Social Studies and Advocacy, stated that the provisions on RTBF in Indonesia found in both the UU ITE and Law Number 27 of 2022 concerning Personal Data Protection are still broad and general. Thus, it poses a significant challenge for the Indonesian government to narrow down and provide proper procedures for RTBF usage in Indonesia.

After examining the comparison of RTBF usage above, it is evident that Indonesia lags behind in several aspects. To find an RTBF model from the four countries that is suitable for implementation in Indonesia, several components must be considered first (Ferraro, 2019). After conducting research, from the four countries that have regulated RTBF usage in their countries, it turns out that France has the most similar characteristics to Indonesia. Some reasons can be mentioned, such as: (1) France follows the civil law legal system, (2) France applies an inquisitorial legal procedure, (3) France is a country that adheres to the ideology of democracy (Whyte, 2020). These three aspects are also applied in Indonesia, so it can be concluded that the implementation of the RTBF legal concept in France will not be significantly different when applied in Indonesia because France and Indonesia share many

similarities in their concepts of governance. Therefore, implementing the RTBF concept from France in Indonesia will only require slight adjustments compared to implementing RTBF from other countries. France has clear procedures for implementing RTBF in their regulations, has a separate authority outside the police with the authority to follow up on cases of personal data misuse, and has sanctions against electronic system providers who refuse to remove an individual's personal data after an RTBF request has been made. These provisions are expected to combat the legal ambiguities or legal vagueness regarding the implementation of RTBF in Indonesia, thereby achieving more comprehensive and effective legal protection for personal data in Indonesia.

## CONCLUSION

In conclusion, Indonesia, particularly under the Information and Electronic Transactions Law (UU ITE), has not explicitly addressed or officially acknowledged the Right to be Forgotten (RTBF) concept as adopted by the European Union through the General Data Protection Regulation 2016 (GDPR), although it is mentioned in Article 26 (3) and Article 26 (4) of UU ITE. Some examples of cybercrimes where the Right to be Forgotten may be relevant are limited to Spreading harmful private information, Defamation, and Copyright Violation. Furthermore, the types of personal data eligible for removal based on the Right to be Forgotten (RTBF) can also be found in Article 4 of Law No. 27 of 2022 concerning the Protection of Personal Data (PDP). This law classifies personal data into two categories: specific personal data and general personal data. According to Article 4 Paragraph (2) of the PDP Law, specific personal data that is legally protected includes health data and information; biometric data; genetic data; criminal records; data of children; personal financial data; and other data as prescribed by the legislation. On the other hand, Article 4 Paragraph (3) of the PDP Law defines legally protected general personal data to include name; gender; nationality; religion; marital status; and personal data used to identify an individual.

Secondly, After analyzing the comparison of RTBF utilization mentioned earlier, it becomes evident that Indonesia lags behind in several aspects. To discover an RTBF model from the four countries that can be effectively applied in Indonesia, various factors must be taken into consideration beforehand. Upon conducting research, it becomes apparent that France bears the closest resemblance to Indonesia among the four countries. This can be attributed to several reasons, including: (1) France adopting the civil law legal system, (2) France employing an inquisitorial legal procedure, and (3) France upholding the principles of democracy. These three aspects are also evident in Indonesia, leading to the conclusion that the implementation of the RTBF legal concept from France would entail minimal adjustments when applied in Indonesia due to the shared governance concepts. France has well-defined procedures for RTBF implementation in its regulations, possesses a distinct authority beyond the police with the mandate to handle cases of personal data misuse, and imposes sanctions on electronic system providers that fail to comply with RTBF requests for removing an individual's personal data. These provisions are expected to address legal ambiguities concerning the implementation of RTBF in Indonesia, thereby establishing more comprehensive and effective legal protection for personal data in the country.

## Bibliography

- Adhari, Ade. (2021). *Policy Limitations on the Internet in Indonesia: Perspectives of the Rule of Law, Human Rights, and Comparative Studies*. *Konstitusi Journal* Volume 18.
- Christianto, Hwian. (2020). *The Concept of the Right to Be Forgotten as Fulfillment of the Rights of Revenge Porn Victims Based on Article 26 of the Electronic Information and Transactions Act*. *Mimbar Hukum Journal* Volume 32.

- Craft, S. (2019). *Unpublishing the news: An analysis of US and South Korean journalists' discourse about an emerging practice*. International Journal of Communication.
- D Maietta, Angelo. (2020). *The Right to be Forgotten*. Revista de Estudos Constitucionals Hermeneutica e Teoria do Direito Journal Volume 2.
- Escouflaire, L. (2023). *The RTBF Corpus: a dataset of 750,000 Belgian French news articles published between 2008 and 2021*. Conference on Corpus.
- Ferraro, Matthew. (2019). *Deepfake Legislation: A Nationwide Survey – State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media*. Wilmerhale Journal Volume 1.
- Jamaludin, Ahmad. (2020). *Reconsidering the Presence of the Right to Be Forgotten: Implementation and Potential Threats*. Indonesian Legislative Journal Volume 17.
- Janclute, L. (2020). *The Right-to-Be-Forgotten Between Acculturation and Geopolitics: Developing a Different Thinking on Some Common One-Liners*. SSRN Papers Volume 3.
- Kusna, Itsna Hidayatul. (2019). *Deepfake, New Challenges for Netizen*. Promeda Journal Volume 5.
- Mahmud, Bahar Uddin. (2020). *Deep Insight of Deepfake Technology: A Journal*. Cornell University Journal Volume 5.
- Rahmadani, Karunia Fitri. (2023). *Juridical Analysis of the Regulation of the Right to be Forgotten in Law Number 19 of 2016*. Hukum dan Perundang-Undangan Journal.
- Rey, I. (2022). *RTBF: For democratic public broadcasting*. La Revue Nouvelle.
- Sukmawati, Agustin. (2020). *Impact of Cyberbullying on Adolescents on Social Media*. Alauddin Scientific Journal Volume I.
- Wachter, Sandra. (2019). *A Right to Reasonable Inferences Re-thinking Data Protection Law in the Age of Big Data and AI*. Hein Journal Volume 1.
- Whyte, Christopher. (2020). *Deepfake News: AI-enabled Disinformation as a Multilevel Public Policy Challenge*. Journal of Cyber Policy Volume 5.