"*Hak Untuk Dilupakkan*" Policy Model: Between Right to Be Forgotten and Right to Erasure

Sayid Mohammad Rifqi Noval
Faculty of Law, University of Islam Nusantara, Indonesia
E-mail: sayidrifqi@uninus.ac.id

Article History
Received: 24 June 2019 **Revised:** 29 July 2019 **Published:** 30 September 2019

Abstract
After the enactment of Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) in Indonesia, an assessment of new right was born through the Article 26 of the Act, known as the Indonesian version of the "Right to be Forgotten (RTBF)." As a country that has just regulated this right, a similar concept is applied in the European Union Countries. This paper examines the comparison of the "*Hak untuk Dilupakkan*" model contained in the EIT Law in Indonesia, with the provisions of RTBF based on Directive 95/46/EC which was considered by some legal scholars as the beginning of this concept, begins to grow and is widely known, and right to erasure (RTE) contained in the General Data Protection Regulation (GDPR) which is considered to be a new RTBF related policy that came into force in May 2018. The *Hak untuk Dilupakkan* model is not entirely similar to the concepts of RTBF and RTE. However, the differences that exist between *Hak untuk Dilupakkan*, RTBF and RTE still adhere to the main concept to give the right to someone to submit an effort to erase the related data about him / her who is widely available on the internet.
Keywords: Right to be Forgotten, Right to Erasure, *Hak untuk Dilupakkan*, General Data Protection Regulation

Introduction
It seems right when the public's attention to the internet has gradually shifted. When I look back at the time when the internet was born in 1969, the era when the internet users' focal point was about how the internet was able to share information. However, at present, the focus is increasingly diverted due to the large desire of internet users to be able to delete bad or unwanted information about themselves published on the internet (Owings, 2015).The hope of some people of the presence of a tool that can erase previous information or has the ability to obliviate the information cited in the internet related to someone's personal/historical data gets a bright spot, after the decision on 13 May 2014 from the Court of Justice of the European Union (CJEU) adjudicating the Google Spain v AEPD case and Mario Costeja Gonzales states that there is RTBF in the context of data processing on the search engine site. The case was submitted by Mario Costeja Gonzales, after his attempt to erase information about the auction event for his house in 1998 was found on a La Vanguardia newspaper website, which is the newspaper with the most readers in Catalonia (Kampmark, 2015).
The court's decision has made RTBF as one of the themes discussed by legal scholars. It did not stop at the RTBF concept, in 2016 the EU launched the GDPR in which there was a so-called RTE, which by some legal scholars were considered to have a close relationship with the RTBF concept and would take effect in May 2018. Both concepts, both RTBF and RTE seemed to have

an inspiration for the State of Indonesia to have a policy with a similar concept. This can be seen in the provisions stipulated in Article 26 of the EIT Law, which became known as the "*Hak untuk Dilupakkan"* (Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions).
However, whether RTBF, RTE and the "*Hak untuk Dilupakkan"* are policies that are completely the same, so that they only leave the issue of terminology, or there are differences in them and whether the rights policy to be implemented in Indonesia has learned from experiences of implementing RTBF and RTE which were previously applied.

Research Method

This study choosea both the descriptive-evaluative and descriptive approaches in analyzing the method. With its descriptive nature, this study would like to provide a number of explanations regarding the background of the presence of the RTBF Concept based on Directive 95/46/EC, RTE based on GDPR, and "*Hak untuk Dilupakkan*" based on the EIT Law. While the evaluative approach is intended so that this study is able to provide an explanation of several legal issues that have the potential to be present in the implementation of " *Hak untuk Dilupakkan* " in Indonesia based on differences in the concepts and practices of RTBF and RTE implementation in EU countries. Whereas prescriptive approach aims to put this study as an instrument to get suggestions and solutions about what should be done, in the framework of preparing policies related to the implementation of the right to be obliterated, in order to reduce potential problems in efforts to implement these policies and in line with the development of RTBF and RTE.

Result and Discussion

Some of the literature found by the author often places RTBF and RTE as different terms but both of them have one meaning, so the presence of "or" (/) and parentheses are always placed between the two terms. This can be seen in research report released by the Global Legal Research Center, The Law Library of Congress (Gesley, 2017) when writing that ".... The Right to Erasure (The Right to be Forgotten)..." or the writing of Bruno Zeller, Leon Trakman, Robert Walters and Sinta Dewi in the European Human Rights Law Review who wrote "..., is the right to be forgotten (otherwise known as the right to erasure) (Zeller, 2019), even the writing of the title of Art. 17 of GDPR is "Right to erasure ('right to be forgotten')". In the initial diagnosis, the author considers that the similarities between the two terms still make a difference to them, so that in this paper a discussion will be conducted separately on the two terms, until finally we must face the fact that the right will be implemented in Indonesia, which is called the Indonesian version of RTBF.

Right to Be Forgotten* Based on *Directive 95/46/EC

The legal concept of RTBF mostly grows in the European Union (EU). One of the discussions on RTBF can be traced in "there is a fundamental right to forget" session at the European Commission's Conference held in May 2009 (Zeller, 2019). Although there have been many discussions about RTBF, actually there is no single definition agreed upon to date. But the general view that is present towards it seems to be in line with Reding's view, namely (Taddeo, 2016):

"if an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system"

Historically in Europe, RTBF has actually received its recognition for a long time, at least according to Frosio it was present when the Court in Europe recognized "right to informational self-determination", a right that was present in relation to the 1983 census of the German state. This right becomes the basis for every individual in Germany to determine the use of the personal data of their citizens (Frosio, 2017).

RTBF is not a new right, the verdict in the case of Maria Gonzales is the fulfillment of basic rights, the right so that the data can be processed fairly for predetermined goals and has obtained the consent of the individual concerned with the data, as well as the rights to give authority to each individual so he/she has access to the data that has been collected about him/her and the right to be able to fix it. This illustrates that RTBF is a derivative of pre-existing right (Hovinheimo, 2016). RTBF received public attention after the submission of deletion of information on search engine results submitted by Maria Costeja Gonzales. The arrears held by Gonzales in 1990 were then published in a local Spanish newspaper which then carried out the digitization process of his articles. Several years have passed, regarding the arrears have been resolved but Gonzales was surprised by the results of the search engine on the Google site when typing his name. The results of the search engine launched the news in the newspaper which again reminded of some of the past events. Until finally Gonzales took the legal route to resolve it. The court further ruled that the search engines are required to remove the search results, when requested by individuals, links to web pages that contain "inadequate, irrelevant or no longer relevant, or excessive" information about that individual (Xue, 2016).

Regarding the term, Callamard uses another option which he thinks is more appropriate for this right, which is de-indexed. Callamard considers that this is the application of Directive 95/46/EC which stipulates that search engine sites are required to delete search results and links to web pages that provide personal information from someone who is inadequate, irrelevant, longer relevant, or excessive. The results of the verdict give authority to anyone in Europe to be able to ask the search engine site to delete a link to a page about themselves, even though the page remains on the Internet (Callamard, 2017). This is what makes searching of archives related to a person difficult to find because it will disappear from the search results of search engine sites, because the search engine sites have indexed the archive. However, if the search for the archive can still be searched with the option to change the typing on the search engine or directly to the original site that has the archive.In the end the implementation of RTBF has become the initial solution to the expectations of internet users for information that they want to eliminate. RTBF also serves as a solution to potential problems caused by anonymity in cyberspace (Li, 2014). Although it is undeniable there are also assumptions if RTBF is considered as a frontal attack on linking, search and archiving. If part of the archive contained on the internet on a media that provides it is removed or makes it inaccessible, the source of historical writing will be lost (Baets, 2016).

***Right to erasure* based on *General Data Protection Regulation* (GDPR)**

In January 2012, The European Union has released its proposal, i.e. General Data Protecting Regulation (GDPR). This document also forms an important policy shift from a "directive" to "regulation". In the European Union legal system, a directive requires harmonizing legislation, a regulation established directly enforceable standards. As Kuner explains, "a regulation leads to greater degree of harmonization, since it immediately becomes part of a national legal system, without the need for adoption of separate national legislation; it has legal effect independent of national law; and overrides contrary national laws (Schwartz, 2013).

The relationship between GDPR and Directive 95/46 / EC regarding data protection can be seen in Recital 9 of the GDPR, i.e.:

"The objective and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity

Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union.

Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law.

Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC"

As pointed out by Recital 9 of the GDPR, These national implementations differed widely, resulting in a complex landscape of privacy laws across Europe. Some member states embraced stricter privacy laws and enforcement while others opted laws and enforcement while others opted for lighter regulation. The GDPR is intended to overcome this situation and harmonize privacy laws throughout the EU. It adopted on May 24, 2016, and its provisions became enforceable on May 25, 2018 (Dageling, 2019).

One of the rules awaited to be implemented by legal scholars is the new RTBF form contained in Art. 17 with the title "right to erasure ('right to be forgotten')". RTE was formulated with the clear view of enhancing data privacy rights for EU citizens (Brimblecombe, 2018). At a glance there are interesting things when the terms RTE and RTBF are coupled, as if both are words that have similar meanings. Napoleon Xanthoulis, perceived that if the two terms are adopted in the interpretation of EC Communication, then the RTBF is tautologous with the RTE or, in Aristotle's terms, both of them constitute things univocally name (Xanthoulis, 2012).

Brimblecombe considered that GDPR introduced a more detailed, comprehensive and explicit RTBF which is known as Right to Erasure. Furthermore, according to him, this RTE will be interesting, because RTE has extra-territorial effect: it will apply to entities based outside the EU that provide services to EU citizens involving the processing of their personal data (Brimblecombe, 2018). Furthermore, according to him, this RTE would be interesting, because a similar view was expressed by Burri and Schar that RTE extends the existing right under Article 12(b) of the Data Protection Directive. In particular, a data subject can now have her personal data erased and no longer processed, where the data is no longer necessary in relation to the purposes for which it was collected; where a data subject has withdrawn her consent or object to the processing of personal data concerning her; or where the processing of her personal data is otherwise contrary to the regulation. Article 17 (3) and Recital 65 put this right into context and clarify that it is not absolute (Burri, 2016). Furthermore, the material scope of Article 17 of the GDPR may thus be broader than that of the RTBF as Article 17 is purported to apply to any instance of online personal data, thus going well beyond search results. Its personal scope may consequently be broader as well, as the burden of erasure would be fostered upon a wider range of online intermediaries, including social media, news websites, content providers and hosting providers (Reymond, 2019).

The provisions related to RTE more fully can be seen in Art.17 (1), (2) and Recital 65 GDPR, i.e.:

1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
    a) The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    b) The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point of Article 9(2), and where there is no other legal ground for the processing;
    c) The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
    d) The personal data have been unlawfully processed;
    e) The personal data have to be erased for compliance with a legal obligation in Union or member state law to which the controller is subject;
    f) The personal data have been collected in relation to the offer of information society services referred to in Article 8(1)
2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Recital 65 GDPR, i.e.:

"A data subject should have the right to have personal data concerning him or her rectified and a ***'right to be forgotten'*** *where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject.*

In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation.

That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet.

The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.

However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims."

When looking at the above conditions, it seems that what is stated by Zanfir is true if Art. 17 GDPR does not create a new right, but it clarifies and strengthens the right to erasure. It does not even mention the derivatives of the verbs "to forget" or "to be forgotten" (Zanfir, 2015). Even though in Recital 66 of GDPR, it was mentioned that:

"to strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request."

There are some provisions that have received serious attention from many parties related to the presence of fines stipulated in the GDPR and includes RTE-related violations. In general, these provisions are regulated in Article. 83 of GDPR and stated in more detail in Paragraphs (4) and (5), i.e.:

4) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
    a. The obligations of the controller and the processor pursuant to Article 8, 11, 25 to 39 and 42 and 43;
    b. The obligations of the certification body pursuant to Article 42 and 43;
    c. The obligations of the monitoring body pursuant to Artcile 41(4).
5) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total wolrwide annual turnover of the proceding financial year, whichever is higher:
    a. The basic principles for processing, including conditions for consent, pursuant to Article 5, 6,7 and 9;
    b. The data subjects' rights pursuant to Article 12 to 22;
    c. The transfers of personal data to a recipient in a third country or an international organization pursuant to Article 44 to 49;
    d. Any obligations pursuant to member state law adopted under Chapter IX;
    e. Non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

***"Hak untuk Dilupakkan"* in Indonesia**

Process of amending Law No. 11 of 2008 on Electronic Information and Transactions, which has now been ratified as Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, is a new right known as the "*Hak untuk Dilupakkan*." The aforementioned rights are the result of adoption of RTBF and RTE which were first born and are valid in the European Union States. The policy regarding *Hak untuk Dilupakkan* can be seen in Article 26 paragraphs (3) and (4) of Law ITE No. 19 of 2016 namely:

3) Each Electronic System Operator must remove Electronic Information and / or irrelevant Electronic Documents that are under its control at the request of the Person concerned based on court determination.
4) Every Electronic System Operator must provide a mechanism for the elimination of Electronic Information and / or Electronic Documents that are irrelevant in accordance with statutory provisions.

Not much information is actually obtained regarding this *Hak untuk Dilupakkan*, given the absence of government regulations explaining further detailed procedures related to the

elimination of information or electronic documents that are deemed irrelevant (Article 26 (5) of the EIT Law).

But there is a view that helps to clarify the irrelevant meaning by doing its interpretation, at least 4 interpretive approaches, namely: (1) textual or grammatical interpretation; (2) systematic interpretation; (3) historical interpretation or original intent of the legislator, and (4) teleological interpretation. Through grammatical interpretation, an understanding that can be understood is information related to information about a particular person. In other words, the limitation of information that can be submitted for deletion is related to a person's personal information. Through systematic interpretation, the limit of irrelevant information that can be proposed is limited to information related to one's personal data, and limited to personal data that is categorized as sensitive, because it must be protected and not allowed to move and use without the consent of the data owner. Furthermore, by using the original intent approach, the purpose of the legislators, the elimination of irrelevant information in question is merely information related to one's personal data. Through the teleological approach, what is meant by the abolition of irrelevant information is limited to information relating to one's personal data, which in the current digital era, is easy to transfer and exchange (Bambani, 2018 (eds)).

Comparison of RTBF, RTE And *Hak Untuk Dilupakkan*

As a real first step, this study can be done by looking at the dominant word meanings used in RTBF and RTE. In RTBF, the word “forget” becomes dominant, and according to Oxford dictionaries it means fail to remember, deliberately cease to think of. While in the RTE, the word “erasure” as contained in the oxford dictionaries contains the meaning of removal of writing, recorded material, or data; the removal of all traces of something, obliteration (Oxford dictionaries). When referring to the meaning of each of the apparent words it feels right if RTBF is considered similar to the term de-indexed because actually this policy does not completely delete the archive from the original site, only removes it from search results from search engine sites like Google. However, if the file is traced to the original site or writes in different words on the search engine site it can still be accessed.

Different when compared to the provisions stipulated in the RTE in GDPR. RTE is not only applied to search engine sites, but is much wider as long as there is data processed by it. So that this is clearly different from the de-indexed process on search engine sites, RTE clearly deletes the main archive by being selectively determined as regulated in Article 17 GDPR. If a comparison is made to *Hak untuk Dilupakkan* in Indonesia. The provisions contained in Article 26 (3) of the EIT Law clearly impose “every provider of electronic systems”. This explains that every organizer of an electronic system that controls the information on its site that is controlled must delete the information, not just search engine sites. Thus, the provisions of the *Hak untuk Dilupakkan* in the implementation target have similarities with the RTE stipulated in the GDPR.

Regarding the data that can be submitted, the court ruling on the Costeja case explains that only personal data can be submitted for RTBF requests by considering if the data is assessed as inadequate, irrelevant, no longer relevant, or excessive. In line with RTBF, RTE also seems to limit itself only to personal data but with a more measurable structure, as stipulated in the Article 17 of GDPR, including: (1) The personal data is not necessary in the context of the purpose of collection and/or processing; (2) Consent to process is withdrawn by the data subject and there is no other legal processing basis. This goes both for consent overall as for explicit consent; (3) The right to object is exercised, in general and in the context of direct marketing IF there are no other legal processing grounds; (4) The processing of the personal data has been done in an unlawful way; (5) The personal data have to be erased for legal obligations to which the data controller is

subject; (6) Processing occurs in the context of children and their personal data collected via information society services; (7) etc. De Terwangne specifically explained the difference between RTBF and Right to Erasure. According to him, the presence of Right to Erasure has reduced RTBF. Right to Erasure gives authority to the subject of data to limit and stop the use of personal data that is not in accordance with legal provisions, while RTBF has stronger protection, because it gives authority to limit the use of personal data with two events, namely (1) withdrawal of consent, and (2) objecting to processing of data (Stupariu, 2015). A different matter is actually shown in the *Hak untuk Dilupakkan* which gives a broader arrangement, namely that all electronic information and / or electronic documents that are irrelevant can be requested. This is an interesting provision, when RTBF and RTE limit which information can be submitted and very carefully give an analytical knife to assess it, *Hak untuk Dilupakkan* instead takes a contrasting step by expanding the information that can be submitted with such a simple "analysis knife", namely "irrelevant", a word that has a high level of relativity and subjectivity, even though there are studies that interpret that meaning.

Related to the scope of its implementation. RTBF as a decision on Costeja only applies to the territory of his country not to all Google branches outside his country (although in its development it has undergone changes, by extending the territory in general (Schwartz Mathew)). While GDPR reaches a wider, extra-territorial effect. GDPR is attached to all companies that process European Union citizen data, regardless of which country the company originates from. A concrete example of implementing this provision is being experienced by Facebook and Google, which is being sued for about $ 8.8 billion dollars by Austrian privacy activist Max Schrems (Brandom). Not as clear as RTBF and RTE, given the absence of government regulations on the *Hak untuk Dilupakkan*, the initial analysis of this provision seems to only apply to providers of electronic systems in the territory of Indonesia.

Regarding excluded reasons, the Costeja case explained that RTBF was not absolutely valid, but not exactly what restrictions were used as benchmarks. But Google specifically explains the reason why the RTBF application was not done, namely by (Google):

"A few common material factors involved in decisions not to delist pages include the existence of alternative solutions, technical reasons, or duplicate URLs. We may also determine that the page contains information which is strongly in the public interest. Determining whether content is in the public interest is complex and may mean considering many diverse factors, including—but not limited to—whether the content relates to the requester's professional life, a past crime, political office, position in public life, or whether the content is self-authored content, consists of government documents, or is journalistic in nature."

Specifically, the GDPR has outlined how the restrictions are made on RTE, as stipulated in Article 17 (3) of GDPR namely:

3) Paragraph 1 and 2 shall not apply to the extent that processing is necessary:
    a. For exercising the right of freedom of expression and information;
    b. For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    c. For reason of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Artcile 9(3);
    d. For archiving purpose in the public interest, scientific or historical research purposes or statistical purpose in accordance with Article 89(1) in so far as the right referred to in

paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e. For the establishment, exercise or defence of legal claims.

While exceptions have been regulated and reported regarding RTBF and RTE, the *Hak untuk Dilupakkan* seems to be awaiting further arrangements. Meanwhile the ELSAM study helps by describing any information that can be submitted for deletion, namely: (1) population information; (2) medical history information; (3) financial, banking and taxation information; (4) information about one's personal self, especially relating to decency, including in relation to child protection; and (5) information that contains slander content against someone, which has been proven to be defamatory according to a court decision that has permanent legal force (Bambani, 2018 (eds)).

Regarding the application mechanism, after the RTBF case, Google provided a channel for every European citizen to submit it directly, the same thing was also implemented by the GDPR which charged every company to accommodate the request. The contract is re-applied to the application for the *Hak untuk Dilupakkan*, which requires the application through the mechanism of a court decision.

Conclusion

After seeing a different side between RTBF and Right to Erasure, both of them still have similarities, namely, intended to something that someone wants to delete, hide or consider so that it cannot be re-accessed (Mantelereo, 2015), similar things also apply to the *Hak untuk Dilupakkan* who adheres to the main goal so that someone has the right to ensure information about him gets protection when published on the internet, especially to be eliminated. In practice, the application of RTBF based on Directive 95/46/EC only gives EU citizens the right to remove search results of themselves from search engine site, but the information archive remains on the original site. This is considered to provide a balance, because the data can still be accessed, but the distribution is limited (Lageson, 2017), with a narrow boundary of regional application and measurable indicators namely inadequate, irrelevant, no longer relevant, or excessive. While the RTE in the GDPR has been very well regulated, such as the determination of the extra-territorial effect, what information can be submitted, the reasons for exclusion and the presence of sanctions for violations. While the *Hak untuk Dilupakkan* in Indonesia tends to try to be able to resemble RTBF and RTE, it is unfortunate to extend the information submitted and not give a good indicator of the reason for the application to be an important note prepared to be present in the mandated government regulation to attend to complete it.

Acknowledgments

This study was funded by the Ministry of Research, Technology and Higher Education of the Republic of Indonesia (Kemenristek-dikti RI). The views expressed are those of the authors and do not necessarily reflect the views of the Kemenristek-dikti RI.

References

Baets, A. 2016. “A Historian’s View on The Right to be Forgotten.” **International Review of Law, Computers & Technology** 30 (1-2): 57-66.

Bambani, A. (eds). 2018. **Hak atas Penghapusan Informasi di Indonesia: Orisinalitas dan Tantangan dalam Penerapannya.** Jakarta: LBH PERS.

Brimblecombe, F. & Phillipson, G. 2018. “Regaining Digital Privacy ? The New ‘Right to be Forgotten’ and Online Expression.” **Canadian Journal of Comparative and Contemporary Law** 4 (1): 1-66.

Brandom, R. 2018. **Facebook and Google hit with $ 8.8 billion in lawsuits on day one of GDPR.** Retrieved from www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe.

Burri, M. & Schar, R. 2016. “The Reform of the EU Data Protection Framework; Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy.” **Journal of Information Policy** 6: 479-511.

Callamard, A. 2017. “The Control of “Invasive” Ideas in a Digital Age”.” **Social Research: An International Quarterly** 84 (1): 119-145.

Dageling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. 2019. **We value your privacy…Now take some cookies: Measuring the GDPR’s impact on web privacy.** (A paper presented in the Network and Distributed System Security Symposium 2019).

Frosio, G. 2017. “The Right to be Forgotten: Much Ado About Nothing.” **Colorado Technology Law Journal** 15 (2): 307-336.

Gesley, J. 2017. “European Union.” In **Laws on Erasure of Online Information.** Retrieved from www.loc.gov/law/help/erasure-online-info/erasure-online-information.pdf.

Hovinheimo, S. 2016. “Legal Subjectivity and the ’Right to be forgotten’: A Rancieran Analysis of Google.” **Law and Critique** 27 (3): 289-301.

Kampmark, B. 2015. “To Find or be Forgotten: Global Tensions on the Right to Erasure and Internet Governance.” **Journal of Global Faultlines** 2 (2): 1-18.

Lageson, S. 2017. “Crime Data, the Internet, and Free Speech: An Evolving Legal Consciousness.” **Law & Society Review** 51 (1): 8-41.

Li, X. 2014. “Phenomenal Exploration into Impact of Anonimity on Law and Order in Cyberspace.” **Kriminologija I Socijalna Integracija** 2 (2): 102-123.

Mantelereo, A. 2015. “The Protection of the Right to be Forgotten: Lesson and Perspectives from Open Data.” **Contratto e Impressa/ Europa** 2: 734-743.

Owings, L. 2015. “Right to be Forgotten.” **Akron Intellectual Property Journal: Akron Law Journal** 9 (1): 3.

Reymond, M. 2019. “The Future of the European Union ‘Right to be forgotten’.” **Latin American Law Review** (2): 81-98.

Schwartz, P. 2013. “The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures.” **Harvard Law Review**126: 1966-2009.

Schwartz, M. 2018. **Google and EU Fight France Over ‘Right to be Forgotten’.** Retrieved from www.bankinfosecurity.com/google-eu-fight-france-over-right-to-be-forgotten-a-11485.

Stupariu, I. 2015. **Defining the Right to be Forgotten: A Comparative Analysis Between the EU and US.** Thesis, Central European University.

Taddeo, M. & Floridi, L. 2016. “The Debate on the Moral Responsibilities of Online Service Providers.” **Science and Engineering Ethics** 22 (6).

Xanthoulis, N. 2012. **Conceptualising a Right to Oblivion in the Digital Media.** London: University College London.

Xue, M., Magno, G., Cunha, E., Almeida, V., & Ross, K. 2016. “The Right to be Forgotten in the Media: Data-Driven Study.” **Proceedings on Privacy Enhancing Technologies** (4): 389-402.

Zanfir, G. 2015. “Tracing the right to be forgotten in the short story history of data protecting law: The ‘new clothes’ of an old right”.” in S. Gutwirth, R. Leenes, & P. Hert (eds). **Reforming European Data Protection Law**. New York: Springer.

Zeller, B., Trakman, L., Walters, R., & Rosadi, S. 2019. “The Right to be Forgotten-The EU and Asia Pacific Experience (Australia, Indonesia, Japan and Singapore).” **European Human Rights Law Review** 23: 23-37.