Eksplorium *p*-ISSN 0854-1418
Volume 46 No. 1, May 2025: 848–879 *e*-ISSN 2503-426X

Research on GDPR Provisions on the Right to be Forgotten and Policy Implications for Vietnam

Dr. Vo Trung Hau
Binh Duong University, Vietnam
vthau@bdu.edu.vn
ORCID: 0009-0006-3560-4359

Article Received: 21 Feb 2025, Revised: 24 April 2025, Accepted: 03 May 2025

Abstract: Building a personal image on the internet is not merely an external presentation; it also reflects an individual's inner personality traits. Privacy as a control right suggests that an individual has the right to decide on the dissemination and use of information related to themselves. In the context of the digital economy, the right to be forgotten can easily spiral out of control once data is published online, as what often follows is continuous recall and memorization, such as search engines potentially storing or linking to previous versions of websites through caching. This article evaluates the GDPR regulations concerning the right to be forgotten, the European Court of Justice (CJEU)'s judicial perspective on this right, and the European Union's (EU) legal provisions regarding its scope of application. From there, the article offers recommendations for improving Vietnamese law on the right to be forgotten.

Keywords: Right to be forgotten, personal information, GDPR

1. INTRODUCTION

According to R. Clark, DJ Solove and L. Floridi, the development of information technology leads to the emergence of digital identity[1]. With the help of these technologies, a person's digital identity is completed . The concept of "one person - one identity" no longer reflects reality, because personal identity is dispersed, ubiquitous, decentralized and permanent. In the context of data processing lacking transparency, companies often rely on consent to collect almost unlimited data, but users often agree to profiling and transmitting digital identity without really understanding it. P. De Hert analyzes the need to recognize the "right to identity" to deal with the threats posed by the Internet of Things (IoT) . P. De Hert believes that profiling is the most important threat to identity, which facilitates the manipulation of people[2]. At the same time, in the digital economy, technology also gives people the opportunity to control their identity through the legal regulation of the right to be forgotten[3]. N. Andrade notes that: "*the proposed concept of the right to be forgotten is not only meaningful from the point of view of identity protection, but also contributes to the continued development of the modern concept of identity, strengthening the understanding of the anti-theoretical nature of identity*"[4]. Thus, the construction of a personal image on the Internet is not simply an external expression but also a reflection of the inner personality traits of each person. Privacy as control suggests that an

[1] Luciano Floridi (2009), "The Information Society and Its Philosophy: Introduction to the Special Issue on The Philosophy of Information, Its Nature, and Future Developments", The Information Society, page 153; Roger Clarke (1995), The Digital Persona and Its Application to Data Surveillance, The Information Society, page 72; Daniel J. Solove (2004), The Digital Person: Technology and Privacy in the Information Age, New York University Press, page 96.

[2] Paul De Hert (2007), A right to identity to face the Internet of Things, https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf

[3] Paul De Hert (2007), A right to identity to face the Internet of Things, https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf

[4] Norberto Nuno Gomes de Andrade (2012), "Oblivion: The Right to Be Different from Oneself - Reproposing the Right to Be Forgotten", Revista de Internet, Derecho y Política, page 122.

individual has the right to decide on the dissemination and use of information related to his or her personality. In the context of the digital economy, the right to be forgotten can easily get out of hand when data is published online because what follows is often constant repetition and memorization as search engines can store or link to previous versions of web pages through caching.

2. REVIEW OF GDPR'S PROVISIONS ON THE RIGHT TO BE FORGOTTEN

2.1. Overview of the right to be forgotten

In France, the right to be forgotten has been recognized since the 1960s. In the United States, the right to be forgotten began to be known in the 1970s with the case of Briscoe v. Reader's Digest Association[5]. From the beginning, the idea of the right to be forgotten was based on desire to provide a means of effectively addressing the offender's past. A. Mantelero argues that the right to be forgotten arises from the need "*of an individual to be able to determine his or her own life without being continuously or habitually stigmatized because of a the consequence of a particular action performed in the past* "[6].

The right to be forgotten in this case is justified by the right to privacy to avoid things that might be harmful to one's reputation[7]. In the case law of the European Court of Human Rights (EctHR) the right to be forgotten falls within the scope of Article 8 of the Charter of Fundamental Rights of the European Union (CFR) and is result of judicial action. European Union (EU) law recognises the right to data protection as an independent right in Article 16 of the Treaty on the Functioning of the European Union (TFEU), Article 8 of the Charter of Fundamental Rights of the European Union (CFR) and in the case law of the Court of Justice of the European Union (CJEU). The Court of Justice of the European Union (CJEU) has cited in Google Spain case a new fundamental right to justify the right to be forgotten. The Court found that the data subject has rights under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR) for being oblivion as a right to request information that is no longer available to the public by removing the listing from the returned results of a search performed by a link to personal data.

There is no clear concept of the right to be forgotten. Research on the concepts of the right to be forgotten shows that in order to understand this right, it is necessary to determine what determinants are included in the concept. Currently, there are two schools of thought that consider different scopes of the right to be forgotten. The first school considers the right to be forgotten as a new right and an extension of the right to erasure. When distinguishing between the right to be forgotten and the right to erasure, P. Bernal argues that the right to erasure as a conceptual basis is more appropriate to how society should perceive personal data on the Internet today[8].

The second school of thought asserts that the Google Spain case never established a new right to be forgotten but simply clarified the scope of the right to erasure without taking into account the case law of the European Court of Human Rights (ECtHR). De Terwangne concluded that the right to erasure and the right to be forgotten are synonymous and that there are three different aspects of the right to be forgotten: (i) the concept of the right to be forgotten in previous judicial practice; (ii) the right to be forgotten established by data protection law.

[5] The California Supreme Court's decision in Briscoe v. Reader's Digest Association, Inc.

[6]Alessandro Mantelero (2013), The EU Proposal for a General Data Protection Regulation and the Roots of the " Right to Be Forgotten ", Computer Law and Security Review, p. 229.

[7] Meg Leta Jones and Jef Ausloos (2013), The Right to Be Forgotten Across the Pond. Journal of Information Policy, page 23.

[8] Paul Alexander Bernal (2011), A Right to Delete?, European Journal of Law and Technology, page 5.

This aspect defines the right to allow data subjects to delete or anonymize their information after the original purpose of the data collection has been fulfilled; (iii) the right to be forgotten in relation to expired data[9]. This interpretation is often considered the broadest interpretation of the right to be forgotten, including the application of an expiry date to data without the need for individual implementation. However, this classification does not cover all possible situations, for example, where an individual is granted the right to delete personal information posted by a third party, even if this information is accurate at the time of publication. The Google Spain case is an example of such a situation. M. Jones and J. Ausloos argue that the right to be forgotten and the right to data erasure are different interpretations of the right to be forgotten[10].

While the right to be forgotten involves the concept of balancing interests to determine when a particular piece of information is no longer relevant to the general public, the right to erasure is more procedural. J. Rosen identifies two situations that fall under the right to be forgotten. The first situation concerns the data subject's right to control, namely the ability to erase information that an individual has posted about themselves. This right is "*widely recognized as a right that is effectively enforceable through contractual terms.*"[11]The second situation concerns the data subject publishing something and someone else copying or reposting this content. Although J. Rosen does not analyze the legality of such data processing, he does assess its compatibility with the General Data Protection Regulation (GDPR)[12].

In particular, whenever an individual requests that their personal information be deleted from an Internet Service Provider (ISP), the Internet Service Provider (ISP) must do so immediately, unless retention of the data is deemed necessary to protect freedom of expression. A third situation involves a third party publishing information about an individual regardless of consent. J. Rosen points out that applying this broad concept could have significant consequences, potentially turning search engines into EU censors rather than neutral platforms[13]. BJ Koops highlights two distinct concepts of the right to be forgotten. The first revolves around the human right to have one's information deleted within a reasonable time and encompasses more strategies that resemble the human act of forgetting. This approach emphasizes the individual's right to control and ownership of that information. According to the second concept, outdated negative information should not be used against people. This view focuses on the whole society rather than on the rights of individuals[14].

Therefore, there is no concept that covers all aspects of the right to be forgotten. When defining the right to be forgotten, it is necessary to focus on the multi-purpose nature and multi-dimensional content of this right. The right to be forgotten is essentially a legal requirement to erase digital behavior left on the Internet in order to protect the individual, his or her dignity, reputation, privacy and identity in the digital economy. Such a concept can include both individual and possible collective claims for the erasure of information. A. Tamo and D. George

[9]Cécile de Terwangne (2013), The right to be forgotten and the Informational Autonomy in the Digital Environment, Publication office of the EU, page 2 5.
[10]Meg Leta Jones and Jef Ausloos (2013), The Right to Be Forgotten Across the Pond, Journal of Information Policy, pp. 2 6.
[11] Jeffrey Rosen (2010), The Web Means the End of Forgetting, New York Times Magazine , http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all
[12] Jeffrey Rosen (2010), The Web Means the End of Forgetting, New York Times Magazine , http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all
[13] Jeffrey Rosen (2010), The Web Means the End of Forgetting, New York Times Magazine , http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all
[14]Bert-Jaap Koops (2013), Forgetting Footprints, Shunning Shadows : A Critical Analysis of the "Right to Be Forgotten" in the Big Data practice, SCRIPTed, page 230.

point out that when deciding to accept the right to be forgotten, countries should start from a broad concept that can be adapted to their own value system [15]. And the right to be forgotten will include "*the practical right to be forgotten and the procedural right to erasure derived from data protection*"[16].

Both the right to be informed and the right to access are expressions of the idea of control over personal data. Another typical instrument of the idea of control over personal data is consent, where consent gives an individual the right to decide whether or not to process data. The right to be forgotten (RTBF) provides the option to review and change the decision about the processing of personal data, even in cases where the processing began without the consent of the data subject. Furthermore, the right to be forgotten (RTBF) also provides the data subject with the ability to influence data processing that has taken place outside the premises of the first data controller. Therefore, the right to be forgotten (RTBF) can be described as one of the strongest expressions of the right to control over personal data. The objective of the right to be forgotten (RTBF) can be related to the idea of information self-determination as a reflection of individual autonomy in the digital economy. The Right to Be Forgotten (RTBF) empowers individuals to take action against data processors – even the most powerful ones such as search engines – by ensuring the right of individuals to decide for themselves whether their personal data should be disclosed or processed. The Right to Be Forgotten (RTBF) can be linked to human dignity by limiting the dissemination of personal data to enhance consumer protection against commercial exploitation of data.

2.2. The judgment of the European Court of Justice (CJEU) on the right to be forgotten

The European Court of Justice (CJEU) plays an important role in the issue of personal data protection because its function is to interpret European Union (EU) law in general and European Union (EU) law relating to personal data protection in particular[17]. In this context, the regulation of the right to be forgotten is entirely subject to the judicial activity of the European Court of Justice (CJEU), which can create a flexible legal framework for this right. However, the Court's interpretation of European Union (EU) law is limited by the large list of cases on which it can base its decision. In addition, the European Court of Justice (CJEU) has shown in its judicial practice that the binding nature of court judgments on the interpretation of European Union (EU) law cannot be understood as having immediate legal effect because they are not final judgments but only preliminary judgments[18].

The judicial practice of the European Court of Justice (CJEU) has not formed a general vision and precision in the development and implementation of the legal framework of the right to be forgotten, but has shaped the scope of the right to be forgotten on a case-by-case basis. Thus, in the Manni case [19], the Court found that the public interest in storing data in a state register was so great that the right to be forgotten was excluded in this case. The Court considered the European Union (EU) data protection rights and Mr. Manni's interest in erasing information about the bankruptcy of his former company in relation to the public interest in

[15]Aurelia Tamò Larrieux and Damian George (2014), " Oblivion, Erasure and Forgetting in the Digital Age ", Journal of Intellectual Property , Information Technology and E-Commerce Law, page 74.
[16]Aurelia Tamò Larrieux and Damian George (2014), " Oblivion, Erasure and Forgetting in the Digital Age ", Journal of Intellectual Property , Information Technology and E-Commerce Law, page 74.
[17]Ondřej Pavelek and Drahomira Zajickova (2019), Personal Data Protection in the Decision-Making of the CJEU
Before and After the Lisbon Treaty, TalTech Journal of European Studies, page 167.
[18]Case C-234/17 Hessische Knappschaft v Maison Singer and sons.
[19] Case C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni

access to information. The Court recalled the fact that the publication of such information in the public register of companies is recognized in law to implement the provisions of the European Union (EU) . The Court ruled that Mr. Manni was not entitled to request the erasure of his personal data because his rights under current data protection law were overridden by the need to protect the interests of third parties in relation to limited liability companies, to ensure legal certainty, the fairness of commercial transactions and the normal functioning of the internal market. Therefore, such disclosure did not result in a disproportionate interference with the fundamental rights of the persons concerned and in particular the rights protected under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR)[20].

The European Court of Justice (CJEU) continues to apply the established judicial practice to the Google Spain case. In 2022, the European Court of Justice (CJEU) ruled on the case of TU and RE v. Google LLC[21]. The case concerned the interpretation of Article 17 of the General Data Protection Regulation (GDPR) . On the one hand, the court clarified the interpretation of Article 17 of the General Data Protection Regulation (GDPR) , expanded the scope of the right to de-referencing links by including photographs and thumbnails, and on the other hand, determined the operator's obligation to conduct its own assessment of the search engine results. European Court of Justice (CJEU) Two questions must be answered in this case[22]: (i) How should the court consider requests to remove links where the applicant claims that information provided by a news agency is inaccurate and where the legality of the publication depends on whether these statements are consistent with reality? (ii) Are search engine providers such as Google required to remove thumbnails from search results, even if the results contain links to the original source?

In its judgment, the Court reiterated that the processing of information by search engine providers should be considered regardless of the content initially published, which is in line with the Google Spain decision and judicial practice[23]. The Court then focused on Article 17.1(a) of the General Data Protection Regulation (GDPR) and reiterated that any restrictions on the right to be forgotten must be provided for by law, respect the nature of the rights, be necessary, proportionate and genuinely serve the purposes of the common interest recognized by[24] the European Union (EU). Although, in the judgment in the GC et al. case,[25] the Court reiterated that as a rule, the right of the data subject to the protection of his or her privacy and data is more important than the right to access information[26]. In deciding whether links to thumbnails in search engine results should be removed within the legal framework of the Data Protection Directive (DPD), the European Court of Justice (CJEU) adopted a similar approach: search engine operators should conduct an assessment when it comes to the use of thumbnails and images, taking into account the added value of public discussion and noting that the protection of personal information is given priority by default. Search engine operators must conduct an independent assessment, taking into account the value of the image for public discussion and taking into account any text accompanying the image.

In addition, the European Court of Justice (CJEU) held that it is not possible to require a search engine operator to proactively verify the information provided by the applicant[27]. But

[20]Case C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni.
[21]Case C-460/20 TU and RE v. Google LLC.
[22] Case C-460/20 TU and RE v. Google LLC, para. 39.
[23]Case C-460/20 TU and RE v. Google LLC, para. 50.
[24]Case C-460/20 TU and RE v. Google LLC, para. 57.
[25]Case C-136/17 GC et al v . Commission nationale del'informatique et des libertés (CNIL)
[26] Case C-460/20 TU and RE v. Google LLC, para. 57 .
[27]Case C-136/17 GC et al v . Commission nationale del'informatique et des libertés (CNIL), para. 70 .

at the same time, it stated that if the person requesting the removal of links presents "*relevant and sufficient evidence to substantiate his request and to demonstrate that the information is manifestly inaccurate*"[28]. The search engine operator is obliged to remove the link to the relevant content. In the event that evidence is presented of the unreliability of the information, the search engine operator is not obliged to remove the links to the results without a court decision.

The judgment also reinforces Google's obligation to verify and provide accurate information. This obligation can be reinforced in the Markets Act (DMA) and the Digital Services Act (DSA) in the United States. The emergence of such an obligation can be viewed in the context of the shift from a liberal understanding of cyberspace[29] to a multi-stakeholder understanding of Internet governance[30]. In this context, the search engine operator must conduct a separate assessment in accordance with established principles that ensure a balance between fundamental rights such as privacy and data protection, freedom of expression, freedom of enterprise, as well as the public interest in access to information and diversity of opinion.

Thus, the consistent implementation of the right to be forgotten by the European Court of Justice (CJEU) in the legal order of the European Union (EU) expands the scope of its application. Although the judgments of the European Court of Justice (CJEU) can be seen as a logical and consistent step in extending the European Court of Justice (CJEU) case law on the right to be forgotten following the Google Spain case. However, this judgment also highlights the lack of a common vision, the lack of an appropriate legal framework to define the scope of the right to be forgotten.

In 2012, when proposing a reform of data protection law, the European Council (EC) declared the right to be forgotten (RTBF) as an independent right and the first pillar of information control[31]. Specifically, the first version of the General Data Protection Regulation (GDPR) stated that the main purpose of the right to be forgotten (RTBF) was to protect children from the negative effects of their reckless behavior on social networks[32]. The right to be forgotten (RTBF) is one of the most notable parts of the European Council (EC) proposal, although it is not a new legal concept[33] because the Data Protection Directive (DPD) already includes the principles of the right to be forgotten (RTBF)[34]. Except for the provision on some new obligations for data controllers and a clearer expression of the right to be forgotten, the proposals of the General Data Protection Regulation (GDPR) are more symbolic than substantive[35].

---

[28]Case C-136/17 GC et al v . Commission nationale del'informatique et des libertés (CNIL), para. 72 .

[29]John Perry Barlow (1996), A Declaration of the Independence of Cyberspace, https://www.eff.org/cyberspace-independence

[30]Richard Hill (2016), "Internet Governance, Multi-Stakeholder Models, and the IANA Transition: Shining Example or Dark Side?", Journal of Cyber Policy, page 176.

[31] Viviane Reding, Your data, your rights: Safeguarding your privacy in a connected world , http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm

[32] European Commission (2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) .

[33] Christopher Kuner (2015), The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines, http://eprints.lse.ac.uk/61584/

[34]European Commission, Factsheet on the "Right to Be Forgotten" ruling, http://europa.eu/rapid/press-release_MEMO-17-1441_en.pdf .

[35]Voss G and Castets-Renard C (2016), Proposal for an International Taxonomy on the Various Forms of the "Right To Be Forgotten": A Study on the Convergence of Norms, Colorado Technology Law Journal, page 290.

According to Article 17(1) of the General Data Protection Regulation (GDPR), the data controller is obliged to erase personal data immediately upon request of the data subject in certain cases: (i) if the subject has withdrawn his consent or objected to the processing of the data; (ii) if the data is no longer necessary for the purpose for which it was collected; or (iii) if the processing of the data is unlawful. The right to erasure can be used against any data controller, i.e. a person or organization that determines the purposes and means of data processing. The right to erasure is based on the exclusive concept of privacy and provides the data subject with the opportunity to withdraw the consent granted to the data controller for the use of his or her data. The scope of Article 17 of the General Data Protection Regulation (GDPR) is much broader than that defined by the European Court of Justice (CJEU). raised in the Google Spain case when it is not limited to search engines but covers all personal information and provides protection not only in the case of requests for irrelevant information from the past but also in other situations such as unlawful processing or withdrawal of consent[36].

2.3. European Union (EU) legal provisions on the scope of application of the right to be forgotten

2.3.1. GDPR provisions on territorial scope of application

The territorial scope of legal frameworks in the digital economy is the subject of much debate. The difficulties in management are mainly related to the unlimited nature of information flows and the development of data processing technologies. With the application of the General Data Protection Regulation (GDPR), the issue of territorial scope becomes more urgent due to the rather broad definition in Article 3 of the GDPR. This is primarily intended to prevent data subjects from being left unprotected[37]. A clear definition of the scope of the GDPR to ensure the effective regulation of the relevant legal relationships will be crucial for the applicability of the right to be forgotten. Article 3 of the GDPR divides the territorial scope into the following situations: (i) According to the criterion of establishment in the European Union (EU); (ii) According to the criteria for determining personal goals in the European Union (EU) .

2.3.1.1. General Data Protection Regulation (GDPR) provisions on European Union (EU) domicile criteria

Article 3 of the General Data Protection Regulation (GDPR) establishes a default rule for determining the territorial scope of application of the General Data Protection Regulation (GDPR). According to Article 3.1 of the General Data Protection Regulation (GDPR), the rule applies when data processing activities take place in the context of the activities of a data controller or data processor in the European Union (EU). According to this provision, the following situations can be imagined: (i) the data subject, data controller or data processor is located in the European Union (EU); (ii) the data controller or data processor is located outside the European Union (EU); (iii) the data subject is located outside the European Union (EU); (iv) the establishment of the data controller or data processor is located in the European Union (EU). Situation (i) clearly falls within the scope of the General Data Protection Regulation (GDPR). For situations (ii), (iii), (iv), the application of the General Data Protection Regulation (GDPR) is controversial. Paragraph 22 of the General Data Protection Regulation (GDPR) clarifies that: "*the basis implies efficient and effective operation through a stable organizational structure. The legal form of this organizational structure, whether through a*

[36]Maja Ovčak Kos (2019), The right to be forgotten and the media, Lexonomica, page 195.
[37]Dan Jerker B. Svantesson (2015), Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation, International Data Privacy Law, page 226.

branch or a subsidiary with legal personality, is not a decisive factor in considering whether it is a "effective and practical". This provision is similar to Section 19 of the Data Protection Directive (DPD) which has been referred to in a number of judgments of the European Court of Justice (CJEU). In the Google Spain case, the CJEU found that the US-registered company Google was subject to European Union (EU) law because its search activity was fully related to advertising sales provided by Google's Spanish subsidiary. Since the data processing in this case involved a search business that helped finance the sale of online advertising for Google in Spain, the CJEU held that the processing was carried out "*within the scope of the activities*" of an establishment in Spain. The CJEU upheld the flexible definition of establishment. Thus, in the Weltimmo case,[38] the CJEU indicates that the concept of basis must be interpreted broadly.

The inclusion of the phrase "*within the scope of activity*" clearly underlines the legislator's intention to define the territorial scope in a broad sense. This term implies that the establishment in the European Union (EU) itself is not obliged to actually process personal data or to be directly involved in the processing of personal data. The European Court of Justice (CJEU) has shown that it is not sufficient to simply provide services in a Member State[39]. In the Google Spain case, the European Court of Justice (CJEU) explained that it is sufficient that the activities of an entity within the European Union (EU) are closely linked to the data processing activities of a controller or processor outside the European Union (EU). This criterion is "*closely linked*" and confirms the functional approach to interpreting the territorial scope of data protection. The question of whether data processing activities are carried out in the context of an establishment in the European Union (EU) should be decided on a case-by-case basis. Therefore, Article 3.1 of the General Data Protection Regulation (GDPR) establishes a definition of territorial scope by default.

In theory, anyone outside the European Union (EU) can invoke the data subject rights under the General Data Protection Regulation (GDPR) . The key point in assessing territorial applicability in these situations will be whether the actual processing actions being challenged occurred within the the activities of the controller or processor are within the European Union (EU). The more organisations involved in the processing are located outside the European Union (EU), the more difficult it will be to apply Article 3.1 of the General Data Protection Regulation (GDPR) .

2.3.1.2. General Data Protection Regulation (GDPR) provisions on personal targeting in the European Union (EU)

Article 3.2 of the General Data Protection Regulation (GDPR) defines the situations where the General Data Protection Regulation (GDPR) may apply, even if the controller or processor does not have an establishment in the European Union (EU). This ensures that personal data subjects in the European Union (EU) can invoke the right to erasure of their data in relation to non- EU organisations where these organisations: (i) offer goods or services to data subjects in the European Union (EU); or (ii) collect data relating to individual behaviour that takes place in the European Union (EU) . In fact, the idea of focusing on "personal targeting" has been used in many European jurisdictions[40]. Overall, this provision is certainly consistent with the interpretation of the fundamental right to data protection. The interpretation

[38]Case C-230/14 Weltimmo sro v. Nemzeti Adatvédelmi és Információszabadság Hatóság.

[39]Case C-191/15 Verein für Konsumenteninformation v Amazon EU Sàrl, para. 76

[40]Douwe Korff (2010), New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, European Commission DG Justice, Freedom and Security Report, https://ssrn.com/abstract=1638949

of the territorial scope of this right must be made in the light of effective and comprehensive protection for data subjects.

In the case of the provision of goods and services, controllers and processors established outside the European Union (EU) are subject to the General Data Protection Regulation (GDPR) when they process personal data in connection with goods or services provided to data subjects in the European Union (EU). This means that the right to erasure may still apply to controllers not based in the European Union (EU). Determining whether a controller or processor is actually providing goods or services to data subjects in the European Union (EU) requires a specific approach, taking into account the specific factors of each case. In this regard, the General Data Protection Regulation (GDPR) makes it clear that simply accessing their website or contact information from within the European Union (EU) will not be sufficient[41].

The General Data Protection Regulation (GDPR) also applies to data controllers or processors established outside the European Union (EU) when they monitor the behavior of a data subject within the European Union (EU). This means that a data subject may invoke his or her right to be forgotten in relation to a foreign controller monitoring his or her behavior while surfing the web. It is important to note that Article 3.2 of the GDPR only covers the behavior of a data subject occurring within the European Union (EU) [42]. D. Svantensson argues that "*for a large number of parties involved in the processing of personal data, the court will have to conclude that they target almost every country in the world or not target any country at all*"[43]. He described the approach to where to target as "*a legislator's dream but a judge's and even a lawyer's nightmare*."[44] This situation also undermines the legitimacy of the General Data Protection Regulation (GDPR) .

One of the most controversial issues in the regulation of the right to be forgotten is the territorial scope of its application. Another issue, as Solicitor General Szpunar pointed out in his Opinion on Google v. CNIL, is that the territorial principle is highly contested. It is therefore not surprising that national Data Protection Authorities (DPAs) and courts face serious difficulties in interpreting and applying the right to be forgotten, which is why the European Court of Justice (CJEU) has sent a large number of preliminary requests. The CNIL judgment is seen as a territorial restriction on the right to be forgotten. M. Samonte argues: "*By explicitly restricting the territorial scope of the right to be forgotten, the Court seems to have unintentionally limited the impact and protective effectiveness of this right*"[45]. In the case of Piesczek v. Facebook, the Court ruled that: "*Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the Electronic Commerce Directive), must be understood in the sense that it does not prevent the courts of a Member State from ordering a hosting service provider to delete the prohibited information or to block access to*

[41]Case C-191/15 Verein for Konsumenteninformation v. Amazon EU Sàrl, para. 76 .
[42]Dan Jerker B. Svantesson (2015), Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation, International Data Privacy Law, page 23.
[43]Dan Jerker B. Svantesson (2015), Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation, International Data Privacy Law, page 23.
[44] Dan Jerker B. Svantesson (2015), Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation, International Data Privacy Law, page 23.
[45]Mary Samonte (2020), Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under
EU Law,
https://www.europeanpapers.eu/en/system/files/pdf_version/EP_EF_2020_I_003_Mary_Samonte_00332.pdf

it worldwide within the framework of relevant international law"[46]. R. Webe argues that: "*a clearer picture of the real objective of a new fundamental right is needed. The declaration of the right to be forgotten as such is not enough. It recalls the myth of Pandora's box: Driven by her natural curiosity, Pandora opened the box and all the evils contained therein escaped* "[47]. The issue of the territorial scope of the General Data Protection Regulation (GDPR) has also been left open by the European Court of Justice (CJEU). It is unclear whether the right to be forgotten applies only within the European Union (EU) or not? Does the right to be forgotten apply to search engines outside the European Union (EU)?

By setting new standards for the protection of personal data, the European Court of Justice (CJEU) is forcing any Internet company to comply with the rules set out in this ruling, even if the company actually operates outside the European Union (EU). The Court's ruling will clearly raise questions about the extraterritorial nature of both the right to be forgotten and the General Data Protection Regulation (GDPR) in general. The questions about the interpretation of the Data Protection Directive (DPD) raised in the preliminary ruling were assessed in the light of the General Data Protection Regulation (GDPR) "*to ensure that the court's answer in every case would be useful to another court*" [48]. Thus, the Court dispelled doubts about the possibility of transferring the conclusions of this case to the new case but did not resolve the issue of territorial application of the General Data Protection Regulation (GDPR). The European Court of Justice (CJEU) issued its judgment without any evaluation criteria or guidance for national courts on how to implement this judgment. Y. Padova argues: "*The right to be forgotten continues to be the subject of a judicial review while it is being considered by the very Court that created it, after the French Council of State submitted 11 preliminary questions to the Court of Justice of the European Union (CJEU)*"[49].

The European Court of Justice (CJEU) faced a dilemma when it had to choose between two options in the CNIL case. One was to recognize the right to be forgotten as universal, ensuring full protection of this right. The other was to recognize the right to be forgotten as not universal, which would reduce the level of protection of this right but would ensure the "digital sovereignty" of states. At first glance, the Court chose the second option. The Court pointed out that many third countries do not recognize the right to be forgotten or "take a different approach" to this right[50]. That is, states can decide to apply the right to information self-determination[51]. But the General Data Protection Regulation (GDPR) has not been clear in defining the scope of the right to be forgotten beyond the territory of the member states[52]. The Court further held that the public interest in access to information varies significantly depending on the third country and therefore the balance of fundamental rights will also vary. There are no appropriate rules and mechanisms to ensure the balance of interests in situations beyond the European Union (EU)[53]. Therefore, the General Data Protection Regulation

[46]Case C-18/18 Glawischnig-Piesczek, para. 55.
[47]Rolf H. Weber (2011), The Right to Be Forgotten: More Than a Pandora's Box?, JIPITEC, page 120.
[48] Case C-507/17 Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), para. 41.
[49]Yann Padova (2019), Is the right to be forgotten a universal, regional, or "glocal" right?, International Data Privacy
Law, page 45.
[50]Case C-507/17 Google LLC v. CNIL, para. 59.
[51]Case C-507/17 Google LLC v. CNIL, para.
[52]Case C-507/17 Google LLC v. CNIL, para. 62.
[53]Case C-507/17 Google LLC v. CNIL, para.

(GDPR) does not impose an obligation on search engines to apply the right to erasure globally[54].

In the Google Spain case, the European Court of Justice (CJEU) concluded that there is no obligation to de-reference all language versions of the search engine[55]. The Court sought to provide the highest possible level of protection for data protection rights, while respecting international relations. Even the Court's best intentions in the matter of international cooperation are undermined when one evaluates a case from the point of view of the effectiveness of the protection of that right. The fact that the right to be forgotten cannot be fully and effectively enforced would create the opportunity for Internet users searching for information outside the European Union (EU) to still access links that do not apply within the European Union (EU). The European Court of Justice (CJEU) was also aware of this fact. The Court pointed out that the purpose of European Union (EU) data protection law is to ensure a high level of protection throughout the European Union (EU)[56]. This means that asserting the legitimacy of only applying the right to be forgotten in a non-universal manner could undermine the European Union's (EU) goal of ensuring a high level of personal data protection.

The European Court of Justice (CJEU)'s approach to the feasibility of a limited application of the right to be forgotten has been recognized by some researchers as a victory for Google for global freedom of expression.[57] J. Daskal argues that "*countries with less liberal views on freedom of speech and expression may create a fenced version of the internet based on arbitrary arguments*"[58]. In the case of Google v. National Commission for Informatics and Liberty (CNIL), an indirect recognition of not requiring the removal of links worldwide but also not prohibiting such behavior can be seen[59]. The European Court of Justice (CJEU) has stated that although nothing in European Union (EU) law can be interpreted as imposing a global right to de-link, national authorities are not prevented from requiring such a broad exercise on a case-by-case basis, unless this is considered to pose a clear threat to the freedom of information of citizens worldwide[60]. "*By leaving open the possibility of extraterritorial de-referencing, the European Court of Justice continues to pursue its hardline post-Snowden stance on data privacy in a way that is likely to transform the data privacy landscape,* " M. Zalnieriute argues[61].

In the digital economy, even access to information specified in search results by Internet users outside the European Union (EU) can have immediate and significant consequences for victims in the European Union (EU)[62]. The European Court of Justice (CJEU) stressed that the French Council of State (FCoS) considered Google to be a single subject when it comes to the processing of data relating to individuals such as French citizens [63]. The Court also

[54]Case C-507/17 Google LLC v. CNIL, paras. 64-65.
[55]Case C-507/17 Google LLC v. CNIL, para. 64.
[56]Paragraphs 10, 11 and 13 of the General Data Protection Regulation (GDPR).
[57]Pam Cowburn (2019), Google win in right to be forgotten case is victory for global freedom of expression https://www.article19.org/resources/google-win-in-right-to-be-forgotten-case-is-victory-for-global-freedom-of-expression/#:~:text=The%20CJEU%20followed%20our%20recommendations,for%20global%20freedom%20of%20expression .
[58]Jennifer Daskal (2019), Speech across borders, Virginia Law Review, page 66.
[59]Case C-507/17 Google LLC v. CNIL, para. 72.
[60] Case C-507/17 Google LLC v. CNIL, para. 72.
[61] Monika Zalnieriute (2020), Google LLC v. Commission nationale de l'informatique et des libertés (CNIL). American Journal of International Law, page 87.
[62]Case C-507/17 Google LLC v. CNIL, para.
[63] Case C-507/17 Google LLC v. CNIL, para. 52.

acknowledged the validity of the argument that the global application of the right to erasure would certainly meet the declared objective of the General Data Protection Regulation (GDPR) of ensuring a high level of protection for personal data in a global online environment that facilitates the flow of information across national boundaries to an unprecedented extent[64]. P. Dixit argued that: "*The ruling in Google's favour, which only allows dereferencing within* the European Union (EU) *and not globally, has been criticised, however, the ruling in its declaration essentially allows Member States to weigh the right to be forgotten against the right to freedom of information and if in the national public interest there is a reason to request dereferencing globally, then this request can be made. This demonstrates that there is no blanket ban and restriction on the right to be forgotten within the EU* "[65]. In addition, the Court held that Google's data processing across all its domains falls within the scope of the General Data Protection Regulation (GDPR). The Court ruled that Google's data processing should be considered as carrying out a single act of processing personal data rather than multiple separate acts[66]. Although the Court considered that European Union (EU) law does not provide for a global obligation to revoke references, it nevertheless pointed out that the European Union (EU) legislature has the competence to establish the obligation if it chooses to do so[67].

2 .*3.2. General Data Protection Regulation (GDPR) provisions on personal data*

According to Article 4(1) of the General Data Protection Regulation (GDPR) personal data is: "*any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*". Many researchers have criticized the legislative concept of personal data for its unreasonable scope. P. Schwartz and D. Solove argue that absolute and irreversible anonymity is no longer possible today and propose to protect personal data according to a protection threshold but with a clearer definition, namely based on the identified identification risk and to process information in different ways depending on the level of identification[68]. Without understanding what personal data is, it is impossible to determine which data can be deleted or forgotten.

2.3.2.1. General Data Protection Regulation (GDPR) provisions on any information

Any information regardless of its nature, content or format can represent personal data regardless of the medium or form it can be "*letters, numbers, graphics, photographs or sounds*" depending on other criteria for determination. Information does not necessarily have to relate to private or family life and can relate to a person's life, occupation and other qualities of that person. The concept of information has many different meanings and adopting such a broad approach to information will make the concept of personal data widely applicable and

[64] Case C-507/17 Google LLC v. CNIL, paras. 54-58.
[65]Priyanshi Dixit (2019) . Will The Internet Remember You Forever? Right To Be Forgotten And Its Territorial Limits
https://www.iiprd.com/will-the-internet-remember-you-forever-right-to-be-forgotten-and-its-territorial-limits/
[66] Priyanshi Dixit (2019) . Will The Internet Remember You Forever? Right To Be Forgotten And Its Territorial Limits
https://www.iiprd.com/will-the-internet-remember-you-forever-right-to-be-forgotten-and-its-territorial-limits/
[67] Priyanshi Dixit (2019) . Will The Internet Remember You Forever? Right To Be Forgotten And Its Territorial Limits
https://www.iiprd.com/will-the-internet-remember-you-forever-right-to-be-forgotten-and-its-territorial-limits/
[68]Paul M. Schwartz and Daniel J. Solove (2011), The PII Problem: Privacy and a New Concept of Personal Identifiable Information, New York University Law Review, page 50.

interpreted, depending on other conditions. The meaning of the term "any information" was first considered in the Nowak case. The European Court of Justice (CJEU) has ruled that the term reflects the intention of the European Union (EU) legislature to: "*designate a broad scope of the concept of personal data, which is not limited to sensitive or private information, but is likely to include all types of information, not only objective but also subjective, in the form of opinions and assessments*"[69].

The practice of the European Court of Human Rights (ECtHR) also shows that personal data is protected. For example, the European Court of Human Rights (ECtHR) has shown that human DNA or human cell samples[70] contain a large amount of unique personal data [71]and simply storing it constitutes a violation. In other words, even storing this data without any processing or interpretation constitutes a violation of human rights.

2.3.2.2. Provisions of the General Data Protection Regulation (GDPR) regarding

"Related to" is one of the elements of the definition of personal data that requires contextual assessment. To be considered personal data, the question of whether the information is related to a person must first be answered, and even before an analysis of the ability to identify is carried out. "Information related to" an individual can be interpreted broadly or narrowly, and it is important to assess what type and extent the information is connected to an individual, as well as whether this connection exists. The General Data Protection Regulation (GDPR) does not provide any guidance on how to interpret "related to". The phrase "related to" is important in order to work out exactly what relationships or links are important and how to distinguish them. In some cases, the connection is obvious, while in others it is not . Especially when the information relates to an object, for example, the value of a house or a process or event that requires human intervention.

The meaning of the word "relevant to" becomes even broader if we consider that these three conditions are sequential rather than simultaneous. Information is relevant to a person when it is addressed directly to that person or relates to that person's personality, actions, characteristics or life experiences. However, even information that is not related to anyone in any way can become "relevant to" a person. Information is relevant to a person "*when the data is used or is likely to be used for the purpose of assessing, processing in a certain way or influencing the condition or behaviour of an individual.*" or where "*its use is likely to have an impact on the rights and interests of a person*"[72]. Furthermore, such an impact is considered sufficient "*if that individual may be treated differently from others as a result of the processing of that data"*[73]. It is worth noting that the connection between purpose and outcome will occur not only when the data has been used, but also when the data is likely to be used for a purpose or to have an impact on people, "*taking into account all the circumstances relevant to the particular case*"[74]. In this context, a broader scope of identification is used than the standard of Section 26 of the General Data Protection Regulation (GDPR) .

[69]Case C-434/16 Peter Nowak v. Data Protection Commissioner, para 34 .

[70]Cases 30562/04 and 30566/04 , S. and Marper v. The United Kingdom , para 50.

[71] Cases 30562/04 and 30566/04 , S. and Marper v. The United Kingdom , para 75.

[72]Nadezhda Purtova (2017), The law of everything. Broad concept of personal data and future of EU data protection law , Law, Innovation and Technology, page 40 .

[73]Nadezhda Purtova (2017), The law of everything. Broad concept of personal data and future of EU data protection law , Law, Innovation and Technology, page 40 .

[74] Nadezhda Purtova (2017), The law of everything. Broad concept of personal data and future of EU data protection law , Law, Innovation and Technology, page 40 .

In the digital economy, any information can be linked to a specific person for its purpose, and all data can affect a person through various influences. Most information is processed for the purpose of evaluating, influencing the state or behavior of people. For example, regulating communication or influencing human behavior are the main reasons for collecting and processing information on the Internet. Therefore, the term includes information about an individual, even if the information is not directly related to that individual in terms of content, but is related to the purpose or effect of processing that information . However, the judicial practice of the European Court of Justice (CJEU) in the case of YS et al[75]. The Court adopted a restrictive interpretation of the term "relevant to". The Court rejected the understanding of the term "relevant to" in terms of the relationship between purpose and result. It is important to note that this decision does not preclude the use of a broader interpretation of "relevant information" in other situations. This means that, even if the information used for assessment is different from the YS case and similar cases, a broader interpretation may still apply. In Nowak v. Data Protection Commissioner, the Court modified the meaning of the term "relevant information". First, the European Court of Justice (CJEU) confirmed that the concept of "personal data" is capable of including any information if it is "relevant" to the data subject, including information relating to a specific person. according to content, purpose or effect. In the Google Spain case, the Court adopted a broad approach to the control of search engine providers and personal data uploaded to third-party websites[76].

2.3.2.3. The provisions of the General Data Protection Regulation (GDPR) on identified or identifiable

To be considered personal data, information must relate to an "identified or identifiable" person. Article 4(1) of the General Data Protection Regulation (GDPR) explains that a person can be directly or indirectly identified and provides a non-exhaustive list of so-called "identifiers"[77]. It is understood that "identified" refers to a person who is known or distinguished within a group and "identifiable" refers to a person whose identity is not yet known but who can be identified. Paragraph 26 of the General Data Protection Regulation (GDPR) defines reasonable identification , taking into account the level of technological development at the time of processing: "*In determining whether an individual is identifiable, all available methods shall be taken into account reasonably capable , for example , of being used by the controller or another person to identify an individual directly or indirectly. In determining whether the methods are a reasonable means of identifying an individual, account must be taken of all objective factors, such as the cost and the amount of time required for identification, taking into account the technology available at the time of processing and the development of the technology*".

Means of identification "*reasonably likely to be used by the controller or any other person*" are interpreted more broadly to include anyone. This interpretation expands the scope of data that is considered personal data. However, relying solely on hypothetical identification is not enough to meet the "*reasonably likely*" standard. In assessing reasonableness, "*all relevant factors"* should be taken into account. The standard of reasonableness is quite broad, so "*Paragraph 26 of the GDPR makes the GDPR concept of personal data more relevant, using contextual analysis to decide whether personal data is recorded or not* "[78]. The same data may

[75]Case C-141/12 YS et al.
[76]Case C-131/12 Google Spain , para.
[77] Arvind Narayanan and Vitaly Shmatikov (2010), Myths and Fallacies of "Personally Identifiable Information" , Communications of the ACM , p. 24.
[78]Paul M. Schwartz and Daniel J. Solove (2011), The PII Problem: Privacy and a New Concept of Personal Identifiable Information , New York University Law Review, page 50.

be anonymous at the time of collection but later become personal data only by the application of technological advances. Michèle Finck and Frank Pallas argued that the meaningful distinction between identifiable and non-identifiable information is no longer tenable[79]. The Court considered the meaning of the word "*identifiable*" in the Breyer decision. The central issue the Court considered was whether a dynamic IP address represents information relating to an identifiable individual relative to the website provider in cases where additional data necessary to identify the website visitor is held by the visitor's Internet service provider[80]. The Court followed a broad interpretation of identifiable but narrowed the scope of the concept of "*personal data*".

The European Court of Justice (CJEU) concluded that to be considered personal data, it is not necessary that the information must enable the identification of the data subject or that "*all the information enabling the identification must be in the possession of a single person* "[81]. The Court proposed to assess "*whether the possibility of combining a dynamic IP address with additional data held by an Internet service provider constitutes a means reasonably likely to be used to identify the data subject* " [82]. The Court considered the argument of the Solicitor General (AG) that the possibility of combining a dynamic IP address with additional data would not be reasonably likely to be used when it was "*prohibited by law or practically impossible* " due to "*disproportionate effort in terms of time, cost and manpower*" [83]. Web site providers have tools that can be used with sufficient probability to identify Web site visitors based on dynamic IP addresses with the help of third parties, namely Internet service providers and competent authorities[84]. Therefore, dynamic IP addresses are personal data.

2.4. General Data Protection Regulation (GDPR) provisions on the processing of personal data

According to Article 4 (2) of the General Data Protection Regulation (GDPR) , data processing is any operation or set of operations which is performed on personal data, whether or not automated, such as collection, recording, organization, structuring, storage, adaptation or modification, searching, consulting, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The General Data Protection Regulation (GDPR) provides a non-exhaustive list of examples explaining what such operations may entail and there is no distinction between collection and use of information, regardless of the methods used, intensity or frequency of the operations. The European Court of Justice (CJEU) pointed out in the Lindqvist and Google Spain cases that even the most insignificant data processing operations can quickly have a significant impact on the data subject[85]. In the Google Spain case, the Court rejected the argument that Google had given as follows "*cannot considered as processing data appearing on third-party websites displayed in search results lists, since search engines process all information available on the internet without distinguishing between personal data and other information"*[86]. It is important to emphasize that whether an activity directly involves the processing of personal data is not the determining factor. Instead, the scope of data protection

[79]Michèle Finck and Frank Pallas (2019), They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR, International Data Privacy Law, page 36.
[80]Case C-582/14 Patrick Breyer v. Bundesrepublik Deutschland, para.
[81]Case C-582/14 Patrick Breyer v. Bundesrepublik Deutschland, para. 43.
[82]Case C-582/14P atrick Breyer v. Bundesrepublik Deutschland, para. 45.
[83]Case C-582/14 Patrick Breyer v. Bundesrepublik Deutschland, para. 46.
[84]Case C-582/14 Patrick Breyer v. Bundesrepublik Deutschland, paras. 46 - 49.
[85]Case C-101/01 Lindqvist; Case C -131/12, Google Spain , paragraph 24.
[86] Case C -131/12 Google Spain , paragraph 23-24 .

requirements is extended to include actions that do not directly involve the processing of personal data. This approach is particularly evident when considering data protection requirements, as actions such as erasure, encryption or anonymization of personal data are included in the definition of processing. These actions are therefore also covered by the General Data Protection Regulation (GDPR) . The principles of processing are applied by the European Court of Justice (CJEU), the European Court of Human Rights (ECtHR) and the General Data Protection Regulation (GDPR) can be understood as a mechanism to achieve balance through a gradual development process. Because there is a common ground for all actions carried out under the law or grounds for the lawfulness of data processing. By establishing the characteristics of lawfulness, the European Court of Justice (CJEU) has introduced terms such as "*insufficient, irrelevant or excessive in relation to the purposes of the processing*"[87].

In addition, both the European Court of Justice (CJEU) and the European Court of Human Rights (ECtHR) have legalized the processing of data for public use in scientific research or library archives . Public protection is enhanced by allowing data processing while ensuring the exercise of freedom of expression. Civil rights are protected if they are consistent with the principles established by law, meet the fundamental protection objectives and correspond to the values of a democratic society. The provisions of the General Data Protection Regulation (GDPR) clearly define the scope of the lawfulness of the processing of personal data. However, when interpreting the principles of case law arising from both the European Court of Justice (CJEU) and the European Court of Human Rights (ECtHR), it is based on General Data Protection Regulation (GDPR), some principles were abolished when the General Data Protection Regulation (GDPR) was enacted create the current framework .

The General Data Protection Regulation (GDPR) does not consider the protection of individuals as a restriction on the movement of personal data. According to Article 1.3 of the General Data Protection Regulation (GDPR) : "*the free movement of personal data within the Union shall not be restricted or prohibited for reasons of protection of individuals with regard to the processing of personal data*". The European Court of Justice (CJEU) considers the objective of promoting the formation of the internal market in the model applied by the General Data Protection Regulation (GDPR) to be secondary in its practice and gives priority to the objective of protecting the rights of individuals. In the cases of Schrems II[88], Wirtschaftsakademie[89] and FashionID [90], the Court has formulated approaches to the foreseeability of the application and interpretation of the General Data Protection Regulation (GDPR) in the future to protect the rights of individuals. The Court's judgment in Google v. CNIL even allowed the right to be forgotten to continue to apply worldwide and is considered an effort to build progressive case law to protect human rights in the digital economy[91]. The European Court of Justice (CJEU) has been remarkably consistent on the interpretation in the context of the protection of the fundamental right to data protection. This order has not changed since the adoption of the General Data Protection Regulation (GDPR) and in judicial practice since the Google Spain case. The Court's position is therefore that any unintended effects that may result from the broad application of European Union (EU) law on personal data protection should be mitigated by a proportional application of specific provisions in the specific context.

[87] Case C -131/12 Google Spain , paragraph 92-94.

[88]Case C-311/18 Facebook Ireland v Schrems.

[89]Case C-210/16 Wirtschaftsakademie Schleswig-Holstein.

[90]Case C-40/17 Fashion ID.

[91]Case C-507/17 Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)

3. SOME POLICY RECOMMENDATIONS FOR VIETNAM

The General Data Protection Regulation (GDPR) sets out various obligations for data controllers, including measures that can be taken to achieve objectives such as the retention limitation principle, the purpose limitation principle, and ensuring privacy by design. In addition, technical measures include deletion by default, expiration dates, obfuscation, and several other technical solutions. The idea of integrity refers to a situation where any bad or wrong things an individual has done in the past are forgiven or forgotten so that one can start afresh. This idea is close to the goal of the right to be forgotten (RTBF) because outdated and irrelevant data can harm an individual and, therefore, should not be used. When that data is deleted, an individual can start over. Koops envisions how the right to integrity will extend to areas outside data protection law, where people are particularly vulnerable to having harmful information about their past revealed. These context-specific measures aim to control how other parties can use information when making specific decisions affecting individuals[92].

3.1. Recommendations for Vietnam to issue legal regulations on technical measures to remove defaults

Deletion by default is a technical solution to ensure that deletion becomes an inherent part of data processing. By using deletion by default, data use becomes circular, starting with collection and ending with deletion. Deletion by default technologies should be designed so that every data unit disappears. For example, the deletion by default process has been integrated into the popular photo messaging app Snapchat[93]. However, Snapchat should not be taken as a model. Although Snapchat's commercial campaign promoted the privacy of ephemeral posts, it was discovered that Snapchat had not deleted the photos after its successful launch. Although users no longer had access to them, the photos remained on Snapchat's servers[94]. In addition, the automatic disappearance of photos is also challenged by the activities of other Snapchat users. This is not surprising to Snapchat users.

The complex and multi-layered ways in which data is collected affect data subjects and their experience of control. Does the Right to Be Forgotten (RTBF) provide any remedy for the lack of transparency of collected data? The Google Spain case is particularly noteworthy in this regard. The judgment addresses profiling through the combination of search results, a type of data collection that includes both data reuse and the combination of data sets. Deleting search results prevents the creation of misleading profiles and their unrestricted dissemination through search engines. Deleting search results protects individuals in the digital economy better than deleting the original data sources, as it limits the availability of algorithmically generated biased results about an individual. Delisting is an example of an effective application of the right to be forgotten (RTBF) that helps subjects control their data, protecting their privacy and autonomous choice.

Article 17(2) of the General Data Protection Regulation (GDPR) recognises the threats to effective data erasure that arise from the unrestricted sharing and copying of data by third parties. Article 17(2) of the General Data Protection Regulation (GDPR) stipulates that upon

[92]Koops BJ (2011), "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice", SCRIPTed, pp. 25 0.
[93]Michael L Rustad and Sanna Kulevska (2015), Reconceptualising the Right to Be Forgotten to Enable Transatlantic Data Flow, Harvard Journal of Law & Technology, page 390.
[94]FTC (2014), Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False, https://www.ftc.gov/news-events/news/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were-false

an erasure request, the controller must notify all thousands of parties with whom the data has been shared. While this obligation is burdensome for the controller, it does little to help the data subject exercise actual control and effectively implement the right to be forgotten (RTBF).

Data can be collected from many sources and shared widely in the digital economy. Identifying each instance of personal data sharing can be challenging. Second, even if all these parties are reached and respond to the notification, there is no guarantee that the data in their possession will be deleted. The notification obligation does not affect the actual deletion of the data source. Under this obligation, the data controller is only obliged to communicate the information and has no obligations regarding the actual deletion. To avoid the undesirable consequences of uncontrolled and decontextualised data collection, some technical measures similar to the right to be forgotten (RTBF) have also proved useful. For example, information intermediaries such as Google and Facebook provide user control platforms where users can adjust and delete content they do not like. In this way, they alone control what data the platforms should have access to. For example, they can prevent search engines from linking to their social media profiles. However, these tools should be used with some scepticism, as many provide less protection than the legal framework does. However, due to their accessibility and user-friendly interface, they can achieve, to some extent, similar goals to those of the right to be Forgotten (RTBF).

An alternative, neutral solution is obfuscation, the deliberate use of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects. For example, obfuscation software can disguise users' search results and cause bottlenecks in online advertising processes. While obfuscation does not delete data, it does prevent data collection and subsequent reuse. There is no way to find and delete all copies of relevant information, but for most users, only the easily discoverable information is important. The result is similar to the case of the right to be forgotten (RTBF).

The right to be forgotten (RTBF) also applies to personal data processed by algorithms. However, data deletion requests are not easily transferable because AI neither learns nor forgets as humans do. Data deletion in the context of AI is much more complicated. In simple technical terms, data is not deleted but removed from the search index. This can take a long time because databases often add new data rather than search existing space due to performance issues. Since AI remembers and forgets differently than humans, this problem must be solved in an AI-specific way. One proposed solution is to use dropout algorithms, a method of artificial forgetting. This method introduces an additional layer between the learning algorithm and the data on which the algorithm is trained; this layer consists of a small number of summation calculations. Such a design removes any dependencies that each layer has on the other. It allows the system to learn a piece of data without reconstructing the entire model and the relationships between the data. The situation becomes more difficult when algorithms use observational data, especially inferred ones. Inferred data consists of characteristics assigned to a person based on his or her online activities and behaviour.

Typically, this data is inferred from a large group of users. This data type is at the core of data-driven algorithms because it enables predictions, which companies need for various commercial purposes. If just one data subject requests deletion, deleting one person's data will not significantly affect the trained model or algorithmic output. To effectively use the right to be forgotten (RTBF) to change models, entire groups would need to explicitly or implicitly cooperate to request deletion, which is highly unlikely. Even if we ignore the lack of transparency in AI, which prevents users from having any meaningful insight into how algorithms process their information, applying the right to be forgotten (RTBF) to AI and other new technologies is proving difficult. The first example is Google's Right to be Forgotten

(RTBF) system. In principle, personal data is no longer accessible via Google search after a successful deletion request. However, by taking advantage of the design of Google's search engine, the researchers identified 30-40% of the deleted URLs.

This can lead to misuse of data. A second example is backups and data retention. Modern business operations such as advanced data analytics and automated business decisions increasingly rely on backed-up and archived data, including personal data. Backups are essential for uninterrupted business operations and beneficial to data subjects when their data is available promptly. In the context of the right to erasure, erasing backup systems may seem impractical and undesirable from an individual's perspective and technically challenging. User data is not stored in a single system. Instead, it is distributed across multiple applications and repositories, off-site and on-site, and can be found in various forms such as emails, files, and database records. The scope of data protection law limits the oblivion of personal data to prevent unwanted data-based decisions. In short, to retain some control for individuals, the right to be forgotten (RTBF) is unlikely to prove useful. It has had little success in controlling inferred data and is often challenged by new technologies.

The final step in the data value chain is to act on the discovered knowledge, that is, to use the insights from the collected data to make useful decisions that can generate profits. These decisions can be good for the economy and the individual but can also be discriminatory, invasive of privacy, or biased. One of the aims of the right to be forgotten (RTBF) is to limit the use of data that could cause harm to an individual. The restriction, in principle, reduces the risk of unintended and undesirable consequences from data reuse. This is why the purpose limitation principle is included in the grounds for the right to be forgotten (RTBF). Noise should be removed from data processing to avoid corrupting the data set and distorting its interpretation. However, almost any personal data unit can be considered relevant on the increasingly personalised Internet. It will be difficult to convince data controllers that the data should be forgotten because it is no longer necessary for the purpose for which it was originally collected[95].

3.2 Vietnam issues legal regulations on technical measures on expiration dates

The idea of an expiration date for personal data addresses the temporal challenge of digital memory by defining how long information should be kept and remembered[96]. Two approaches can be distinguished: the first is an expiration date for data, and the second is an expiration date for consent. One of the first to advocate expiration dates was Mayer-Schönberger, who argued that introducing an expiration date would make it possible to simulate human forgetfulness in the digital world[97]. This would be done by linking information stored in digital memory to an expiration date that the user sets himself: " *Our digital storage devices will be created to automatically delete information that has reached or exceeded its expiration date"*[98]. Technically, expiration could be implemented by adding additional metadata. Mayer-Schönberger predicts this would not be a major problem for tech companies,

[95]Bart Custers Bart and Helena Ursic (2016), Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection, International Data Privacy Law, page 10.
[96]Michael L Rustad and Sanna Kulevska (2015), Reconceptualising the Right to Be Forgotten to Enable Transatlantic Data Flow, Harvard Journal of Law & Technology, page 383.
[97]Viktor Mayer-Schönberger (2011), Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, page 171.
[98]Viktor Mayer-Schönberger (2011), Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, page 171.

although it could interfere with their established business systems[99]. However, it would require government action, code changes, or strong consumer pressure[100]. One downside to this option is that data subjects need foresight to set the exact date for potentially harmful data[101]. A similar solution would be the idea of a consent expiration date. It would provide similar benefits to a data expiration date because it would create a basis for deleting the data. However, this idea is not without its problems. Custers notes that the expiration date of the consent would require more metadata, "*which could also reveal the data subject's privacy preferences, resulting in less privacy rather than more privacy, since privacy preferences could be used for personalisation or profiling."* [102]

3.3. Vietnam issues legal regulations on technical measures to prevent code obfuscation.

Elena Esposito argues that deleting the information is contrary to the nature of AI. Algorithms do not tend to forget like humans but must be programmed to remember everything. However, by forcing the deletion of history, the most immediate effect is to draw attention to it, thus triggering memorisation. This can be observed when searching on Google for a person that Google has forgotten. Among the results, a warning appears that some content has been deleted under the right to be forgotten (RTBF). The obvious consequence is to increase curiosity and interest in that content[103]. Esposito emphasises that classical information deletion does not work with AI, so a new approach to forgetting is needed, proposing a direct process instead of deleting content or making it unavailable. To reinforce forgetting in the context of AI, memories should not be deleted but multiplied[104]. One technical measure to realise Esposito's idea is code obfuscation, proposed by Brunton and Nissenbaum and defined as the addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects[105]. Code obfuscation targets secondary data processing to prevent the reuse of personal data. Certainly, obfuscation is not a form of deletion but a form of anonymisation. However, they serve similar purposes. Since deletion sometimes does not work, obfuscation can be a good alternative, leading to similar, if not identical, results. Alternatively, demoting can be used. Demoting deliberately places some search results at the bottom of a search engine's results page. This technical solution can also be effective for personal data. It can become an alternative to the right to be forgotten (RTBF), striking a better balance between privacy and freedom of expression. By demoting links with personal data, a person's privacy will still be protected to a large extent. At the same time, the information will still be available to diligent and serious researchers, thereby limiting the negative impacts on freedom of expression.

[99]Viktor Mayer-Schönberger (2011), Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, page 171.
[100]Viktor Mayer-Schönberger (2011), Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, page 171.
[101]Michael L Rustad and Sanna Kulevska (2015), Reconceptualising the Right to Be Forgotten to Enable Transatlantic Data Flow, Harvard Journal of Law & Technology, page 383.
[102]Bart Custers (2016), Click Here to Consent Forever: Expiry Dates for Informed Consent, Big Data & Society, page 12.
[103]Elena Esposito (2017), Algorithmic Memory and the Right to Be Forgotten on the Web, Big Data & Society, page 36.
[104]Elena Esposito (2017), Algorithmic Memory and the Right to Be Forgotten on the Web, Big Data & Society, page 36.
[105]Finn Brunton and Helen Fay Nissenbaum (2016), Obfuscation: A User's Guide for Privacy and Protest, MIT Press, page 15.

3.4. Vietnam issues legal regulations on identification rights

The life of a modern person has another version, which is digital. The digital version increases the pressure on the massive exchange of personal information with the widespread adoption of this platform and the power of media, which has made people more vulnerable[106]. The existence of digital life suggests the need to develop more comprehensive mechanisms to protect individuals in the digital world. Creating or choosing your content for your digital identity involves providing a person with legal tools to create and protect their choices. The law must give a person the confidence to be who he wants. In this sense, a person is a subject who recognises himself as an active subject and tries to control his path in the digital world. The new informational nature of identity makes it a matter of data processing and information management, so many legal mechanisms provided and applied in personal data protection can become legal tools to protect identity. As E. Oreg notes, the broad definition of processing and personal data in the General Data Protection Regulation (GDPR) includes cases of violations of the right to identification[107]. However, the current personal data protection model cannot fully guarantee identity rights in the digital world.

Therefore, this right allows individuals to exercise autonomy in using their data without the intervention of others. However, the General Data Protection Regulation (GDPR) also strictly regulates personal identifiers, including habits and preferences in the processed data. The difference between the General Data Protection Regulation (GDPR) and GDPR is that it protects personal data and data that reflects personal identity. This stems from personal data, especially stored information closely linked to a person's identity[108]. Using personal data as a form of identity reflection requires stronger protection than the usual regulations on personal data protection. It is necessary to consider the theory to explain the protection Of personal data, which is personally identifiable.

N. Andrade considers the right to personal identification to involve controlling and protecting various types of information. Relating to personal identity or part of personal identity. N. Andrade defines the right to personal identity as the right to express difference, uniqueness and uniqueness[109]. The right to identity is expressed and developed as a right that applies to various changes. Moreover, the identity transition between different ontological levels of "being". Thus, the right to identity is the right to acknowledge the attributes of one's identity and the right to be recognised and identified according to these defining characteristics. The right to identity also includes the right to be represented in the way you want, meaning the right not to be misrepresented; the right to delete and renew self-image and identity activities, including the right to be forgotten and the right to have more identity – meaning the right to create, control and maintain different identities in the digital environment[110]. According to P. Bernal, there are three groups of rights considered to constitute “direct identification rights”. “Line” includes the right to create, assert and protect identity, the right to control connections

[106] Lusine Vardanyan et al. (2022), Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity, TalTech Journal of European Studies, page 159.
[107] Elad Oreg (2018), Right to Information Identity, John Marshall Journal of Computer & Information Law, page 39.
[108] Luciano Floridi (2005), The ontological interpretation of informational privacy, Ethics and Information Technology, page 50.
[109] G comes D e A trade and Norberto Nuno (2012), The right to personal identity in the information age: a reappraisal of a lost right, Florence: European University Institute, page 12.
[110] G comes D e A trade and Norberto Nuno (2012), The right to personal identity in the information age: a reappraisal of a lost right, Florence: European University Institute, page 12.

between online identity and the real person behind that identity[111]. P. Bernal argues that those rights form the right to identity, so they should be seen as fundamental principles for constructing rights and legal rules. P. Bernal argues that the right to be forgotten can be directly from rights to online identity[112]. In this sense, rights create opportunities to Select information and data as content will form a person's digital identity, choosing "*what information about someone will be available and accessible*."[113] As well as maintain and control what will be his reputation and dignity. Given the above, each person's right to create their digital identity boundaries can open up a new perspective. Accordingly, Recognising the right to a digital identity is the basis for the right to information self-determination. The General Data Protection Regulation (GDPR) stipulates that individuals must have control over their data and lays the foundation for the recognition of the right to information self-determination; the content of this right may be determined using the General Data Protection Regulation (GDPR) rights, i.e. the rights to be notified, erased, object, restrict processing, portability of data and not be subject to a decision based solely on automated processing. Identifying an individual's digital identity as a fundamental right would mean laying a new foundation for the rights enshrined in the General Data Protection Regulation (GDPR).

Furthermore, the case law of the European Court of Justice (CJEU) also reflects on the right to be forgotten as a right that focuses on the ability to manage a person's digital version. In particular, according to the judgment in the Google Spain case, an individual is granted the right to remove links from the search engine. As can be seen, this ruling provides a person with a tool to control the digital version of their identity. People can control their image in the digital economy by requesting that a search result be deleted if it is considered incorrect. Hence, the right to be forgotten becomes one of the tools for forming digital identities, which underpin the right to information self-determination. Considering the right to be forgotten in this way can expand the scope of application, becoming a fundamental change in how security is applied in the identity determination process. If we broaden our understanding of the right to be forgotten, it could lead to a fundamental shift in how we think about security. Instead of focusing solely on protecting personal identity, we will move towards a new security approach.

Instead of focusing solely on the right to be forgotten (RTBF), protecting personal privacy and identity would significantly enhance human safety in the digital environment. First, it is necessary to consider the balance between the right to be forgotten and freedom of expression and access to information. According to C. Sullivan, the right to identity is more likely to protect people than the right to privacy. This is because, unlike the right to privacy, the right to identity cannot be restricted in the public interest but can only be limited in exceptional cases[114]. P. De Hert emphasises the need to distinguish identity from privacy rights clearly. P. De Hert points out that current privacy rights cannot fully address and protect issues related to personal identity. Recent technological advances are changing the way we perceive personal identity. Therefore, it is necessary to build a new system of balancing interests, going beyond current regulations and protection concepts such as privacy, freedom, autonomy and discrimination[115]. Since the right to privacy protects personal information within the private

[111] Paul A. Bernal (2012), The Right to Online Identity https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143138

[112]Paul A. Bernal (2012), The Right to Online Identity https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143138

[113] Lusine Vardanyan and others (2022), Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity, TalTech Journal of European Studies, page 90.

[114] Clare Sullivan (2009), Digital Identity – the Legal Person? , Computer Law and Security Review, page 54

[115]Paul De Hert (2007), A Right to Identity to Face the Internet of Things,

sphere, it protects against disclosing and withdrawing information from personal life. The right to be forgotten aims to protect against The dissemination of information published in certain circumstances and distorted information about a person and his identity. Therefore, the extension of the right to identity strengthens the application of the right to be forgotten.

In addition, a lot of personal data is contained in publications on social networks or platforms like YouTube. Such information is protected because it is processed For journalistic purposes only and is not covered by the General Data Protection Regulation (GDPR). However, if the right to be forgotten is considered in the context of the right to identification, such an exception may not apply. Suppose information can create a misconception about a person's personality. In that case, that is a difference between the personality conveyed through outdated information and the personality that Individuals who want to express themselves now can exercise the right to be forgotten. The right to be forgotten can be seen as a mechanism of formation and selection. Identity is dynamic and can be continuously modified since the nature of identity changes over time. The European Court of Human Rights (ECtHR) derives the right to identity from interpretation of Article 8 of the European Convention on Human Rights (ECHR). In the case of Tysiac v. Poland, the European Court of Human Rights (ECtHR) acknowledged that private life is a broad term that includes physical aspects and social identity, including personal autonomy, personal development, and establishing and developing relationships with other people and the outside world. The European Convention on Human Rights (ECHR) not only protects the right to privacy by preventing intrusion but also encourages the full development of the individual. This is clearly shown by the right to personal development as part of the right to respect private life. Accordingly, personal development occurs independently and through relationships with others and the world around them[116]. According to C. Sullivan, The European Court of Human Rights (ECtHR) view of personal identity is based on understanding personal identity as a story, a process of constantly creating and recreating your own life story[117].

The right to be forgotten can be extended to the right to self-determination of identity, allowing each person to decide who they are and how they want to be perceived by society. Clearly defining aspects of personal identity, physical and social, is important in each person's development. Each individual has the right to know and control this information, as it directly affects the process of personality formation. Therefore, a democratic society needs to ensure that each person has the right to participate in shaping their future while also having the right to erase parts of the past that they do not want to keep. This demonstrates respect for each individual's freedom to choose information. Andrade points out that since a formal identity can only exist when past identities are forgotten, the right to be forgotten can play an extremely important role, allowing an individual to reconstruct the story of identity with the confidence that past identities will not affect the present[118].

Therefore, modern threats to individuals in the digital world cannot be ignored by applying modern legal frameworks in the context of privacy. The right to be forgotten is closely

https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf

[116]Jill Marshall (2008), Personal Freedom through Human Rights Law?: Autonomy, Identity and Integrity Under the European Convention on Human Rights, Boston: Martinus Nijhoff Publishers, page 93.

[117] Clare Linda Sullivan (2008), Privacy or Identity? , International Journal of Intellectual Property Management, page 102.

[118] Norberto Nuno Gomes de Andrade (2012), Oblivion: The Right to Be Different from Oneself - Repurposing the Right to Be Forgotten , Revista de Internet, Derecho y Política , page 57.

linked to the ability to self-reflect, form one's identity, and present one's true identity to the world. From the perspective of subjective identity, The mechanisms specified in the General Data Protection Regulation (GDPR) are ineffective because they do not help individuals to present themselves to others in the way they wish. However, the right to be forgotten has the potential to become an identity protection mechanism. Considering the right to Forget the focus of personal identity can help find a new balance of interests.

In order to expand the scope of the right to be forgotten and use it as a mechanism to counter the risks of the Internet, it seems more effective to justify this right through the right to personal identity, which would provide opportunities for protection and security after death. Therefore, the right to be forgotten can be defined as a legal requirement to erase digital behaviour left on the Intertor to protect an individual's dignity, reputation, privacy and identity in the digital economy. Such a definition allows the inclusion of individual and collective claims for such erasure.

3.5. Vietnam issues legal regulations on the right to be forgotten after death

People leave behind digital behaviours throughout their lives; after a person passes away, preserving this information contributes to the survival of the deceased person's digital identity. When a person's digital copy, such as an online profile or a virtual avatar, is no longer tied to their physical body, that digital presence is no longer limited by the usual physical laws. This creates a huge gap in understanding humans because the body has always been considered the sole expression of an individual's identity. Today, in the context of the digital economy, personal data itself has become an expression of identity. The biological body may no longer exist, but the emotions, consciousness, actions, and will that have passed still exist and will continue to exist in the digital world as expressions of human identity. As digital expression continues, careful curation of digital content, which can be seen as a rich reflection of you, becomes increasingly necessary.[119]

However, this would not be easy within the current legal framework. General Data Protection Regulation (GDPR) The issue of protecting personal data after death has been left unattended. Paragraph 27 of the General Data Protection Regulation (GDPR) states, "*This Regulation does not apply to personal data of deceased persons. Member States may adopt rules relating to the processing of personal data of deceased persons".* The General Data Protection Regulation (GDPR), therefore, leaves the issue of post-mortem personal data protection to the discretion of the European Union (EU) member states. Furthermore, the GDPR does not require EU member states to introduce special rules in their national legislation to process and protect deceased personal data. Although Article 8(1) of the Charter of Fundamental Rights of the European Union (CFR) provides that "*Everyone has the right to the protection of personal data concerning him or her*." However, there is no direct assertion regarding the protection of rights after death. However, in the Lindqvist case, the European Court of Justice (CJEU) pointed out that "*nothing prevents a Member State from extending the scope of its national law implementing the provisions of Directive 95/46 to matters not falling within its scope, provided that there is no statutory provision preventing this*"[120]. This indirectly allows for post-mortem data protection, subject to the discretion of the European Union (EU) Member States. However, the Internet is a global network and requires more comprehensive regulation in this area. The European Court of Human Rights (ECtHR) has also taken a cautious

[119] Evan Carroll and John Romano (2010), " Your digital afterlife: When Facebook, Flickr and Twitter are your estate,
What is your legacy? ", New Riders Pub, page 98.
[120]Case C-101/01 Lindqvist, para 98.

approach in its judicial practice. In cases such as Jäggi v. Switzerland, the court recognised "*the right of the deceased, arising from human dignity, to protect their remains from interference contrary to morals and customs*"[121].

In the case of Genner v. Austria[122] The court took a more ambiguous approach, stating that "*the expression of insults after the death of the offended person is contrary to basic decency and respect for the human person…and is an attack on the very core of the right to dignity*."[123] In ML v Slovakia, the court considered a specific aspect of the right to be forgotten – its implementation in the event of the death of the party concerned [124]. ML was the mother of a priest convicted of sexual abuse of minors who died after completing his criminal sentence. Three newspapers published articles suggesting that the priest's death may have been due to his previous criminal convictions. ML initiated legal proceedings against the publishers, claiming that the information was baseless and violated her rights and the privacy of her deceased son. The court reviewed the case and found it admissible , considering the violation of both ML's rights and the rights of the deceased relative. The court acknowledged that Article 8 of the European Convention on Human Rights (ECHR) also covers cases where the treatment of the deceased is out of respect for the feelings of the deceased's relatives[125]. The court has traditionally considered the conflict between freedom of expression and privacy protection. However, these criteria must be applied to information relating to the deceased, which may affect relatives' privacy. The court has argued that the right to be forgotten can extend to the deceased, with relatives possibly exercising this right.

European Union (EU) law is often based on the view that when a person dies, they are no longer considered the subject of individual rights. This view holds that the human rights that a person has when alive cease when they die. However, Judge Fura-Sandstrom of the European Court of Human Rights (ECHR), in the case of Akpinar-Altun v. Turkey, took a different view from this view[126]. Judge Fura-Sandstrom held that the State still must respect the dignity and protect the body of the deceased. This means that, in the judge's view, human rights do not completely disappear when a person dies, and the State still has a responsibility to protect those rights. This approach, which is widely accepted in European Union (EU) law, is no longer valid in the face of the development of an online society. The growing gap between a person's online image and that of his or her real-life poses new challenges. This requires finding effective legal tools and measures to protect the human rights of the deceased in the digital space, including the right to be forgotten. In other words, it is necessary to review the current legal regulations to ensure that the rights of the deceased are still respected in the digital world. This is especially important because, in the absence of a legal framework, this issue is left to the discretion of Internet service providers and social media companies, which provide post-mortem data protection policies that are convenient for them. Often, such policies are not formalised in the general terms and conditions. For example, Facebook's policy on inheritance allows account users to turn the deceased's account into a memorial[127]. OkCupid has a policy according to

[121]Case 58757/00 Jäggi v. Switzerland.
[122]Case 55495/08 Genner v. Austria .
[123] Gianclaudio Malgieri (2018), Data Protection and Privacy: The Internet of Bodies, Hart Publishing, page 100.
[124] Case 34159/17 ML sues Slovakia
[125]Case 34159/17 ML v. Slovakia, para. 23.
[126]Case 56760/00 Akpinar - Altun v. Turkey .
[127] Facebook Help Center, About legacy contacts on Facebook, https://www.facebook.com/help/1568013990080948

which a user's subscription to the Service continues indefinitely until the user cancels it[128]. However, in practice, this impedes the deceased's account from being deleted by relatives.

The legal literature has no unified approach addressing posthumous personal data protection issues in the European Union (EU). Proposing a possible solution to posthumous data protection issues, G. Malgieri sees a combination of posthumous privacy and the right of heirs to own the "digital identity" of the deceased[129]. L. Edwards and E. Harbinja advocate the recognition of posthumous privacy[130]. They argue that this is based on the dignity of the deceased, which deserves protection not only in the physical world but also in the digital world. B. Zhao believes that the heirs of the deceased have two rights after death, namely reputation and privacy[131]. Moreover, both are explicitly recognised by European Union (EU) law. EL Okoro argues that there is no need for post-mortem data protection at the level of European Union (EU) law: "*At the EU level, the call for post-mortem personal data will not be welcomed and responded to by all Member States because each country has its own history and traditional beliefs on which its legal system is based* "[132]. V. Mayer-Schoenberger supports a policy of erasing the personal data of deceased Internet users after their death[133]. However, this is not a good solution to the problem since, according to this approach, personal data containing information about a person's contribution to history, science or art should also be erased. In addition, it raises doubts about the viability of digital identity protection mechanisms.

One of the arguments made by opponents of posthumous privacy is that violating privacy does not harm the deceased. They consider violating the privacy of the deceased to be "non-actual injury," given the fact that the deceased cannot protect their personal data or digital identity[134]. However, in J. Feinberg's view, the principle of consequences also includes consequences that occur after someone dies that affect the person related to them, even if he does not know about it[135]. The harm principle can also apply in the digital environment if a person is understood as being affected in their ability to think, learn, and feel by what others say, think, and write about them. Not only while they are alive but also after they die because it damages their reputation, memories, and what others know about them, wherever that information is located[136]. S. Winter said: "*In my life, the different aspects of my personality create more or less cohesion and interaction overall to the state of my reputation (my public persona)*"[137].

The main purpose of the right to be forgotten is to ensure the right not to become a victim of harm. Furthermore, even if the deceased cannot protect his personal property or data,

[128] OkCupid Terms and Conditions, https://okcupid-app.zendesk.com/hc/en-us/articles/23941864418203-Terms-Conditions
[129] Gianclaudio Malgieri (2018), Data Protection and Privacy: The Internet of Bodies, Hart Publishing, page 100.
[130] Lilian Edwards and Edina Harbinja (2013), Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests
of the Deceased in a Digital World, Cardozo Arts & Entertainment Law Journal, p. 83.
[131]Bo Zhao (2016), Posthumous Defamation and Posthumous Privacy Cases in the Digital Age, Savannah Law Review, page 15.
[132] Egoyibo Lorrita Okoro (2018), Death and Personal Data in the Age of Social Media, Tilburg University, LLM Law and Technology, page 48.
[133] Viktor Mayer-Schönberger (2009), Delete: The virtue of forgetting in the digital age, Princeton University Press, page 272.
[134] Stephen Winter (2010), Against posthumous rights, Journal of Applied Philosophy, page 186.
[135]Joel Feinberg (1989), The moral limits of the criminal law - Self-harm, Oxford University Press, page 448.
[136] Stephen Winter (2010), Against posthumous rights, Journal of Applied Philosophy, page 186.
[137] Stephen Winter (2010), Against posthumous rights, Journal of Applied Philosophy, page 186.

this does not mean the harm has no consequences. First, one should not forget regarding surviving relatives: in any case, such a violation causes direct damage to reputation and their interests. The privacy and reputation of the deceased become an integral part of the reputation of their relatives, regardless of whether they wish to be protected. Second, according to KR Smolensky: "*Suppose a person dies, and his neighbours spread defamatory words about him. These comments damage the reputation of the deceased*; *regardless of whether they are alive or not, they cannot be emotionally upset by the statements. The fact that they are unaware of the harm does not mean that harm to the deceased's interests, particularly their reputation, has not occurred*. "[138] E. Oreg supports the recognition of new legal principles of rights information identification that this principle is the human right to be allowed to use the functions of the information platform that allow others to identify and recognise him, as well as remember who he is and what about him[139]. In the context of memory, changes in the way memory works occur in the information society: if human memory has a natural tendency to forget some events over time, evolution and change are meaningful, whereas digital memory does not allow for change, and their memory remains unchanged and frozen in time. With the creation of increasingly large databases available on the Internet through search engines, social memory is expanding and conditioning individual memory. There is now an obligation to remember, as the collective memory of the Internet accumulates every act of human life, turning them into prisoners of the past and challenging the formation of a free personality. This leads to the need for appropriate remedies, such as the right to be forgotten, to protect the privacy and freedom of the individual.

However, eternal memory in the literal sense of the word does not exclude the fact that the personal data of the deceased, which are freely available on the Internet, cannot lose their social significance in the process of changing life circumstances or contain information that is incomplete, inaccurate, unreliable or reliable but defamatory or offensive. In this case, if the publication and disclosure of such information on the Internet occurs in a European Union (EU) member state whose national law does not have special rules on the processing and protection of personal data after death, the memory of a person and his or her identity information will be distorted and violated. D. Sperling argues, "*Although a person may not survive after death, some of his or her rights may still exist*"[140]. K. Smolensky also states that: "*Although it is true that only a small group of rights may survive death and that an even smaller group is protected by law, death does not necessarily sever all rights and, therefore, does not terminate all legal rights. The recognition of legal rights after death gives the deceased an important moral value in the legal system, which would be expected if legislators were motivated to treat the deceased with dignity*"[141]. Using human dignity as the basis for interpreting the right to be forgotten allows us to overcome the barriers to implementing this right because the broad concept of human dignity can protect not only the deceased but also his or her remains.

The concept of the right to be forgotten through human dignity protection reveals important aspects beyond mere "forgetting" in the digital age. It involves protecting a person during their lifetime and after death, including their digital legacy and what remains of their personality in the digital space. The idea of protecting a person's dignity after death is reflected in understanding the concept of "digital remains". They are an integral part of our digital lives, representing aspects of personality that continue to exist even after a person has left. In this

[138] Kirsten Rabe Smolensky (2009), Rights of the dead, Hofstra Law Review, page 102.
[139] Elad O reg (2012), Right to Information Identity, John Marshall Journal of Computer & Information Law, page 153.
[140] Daniel Sperling (2008), Posthumous Interests, Cambridge University Press, page 121.
[141] Kirsten Rabe Smolensky (2009), Rights of the dead, Hofstra Law Review, page 102.

context, attitudes towards "digital remains" require respect and protection, just as respect is given to people themselves for their dignity. The right to be forgotten is conceived through the lens of the right to respect, suggesting the idea of privacy after death. This means that information about a person after they die must be protected and not used or distributed without valid consent.

The principle of protecting human dignity is contained in Article 1 of the Universal Declaration of Human Rights and Article 1 of the Charter of Fundamental Rights of the European Union (CFR). The memory of the deceased can be protected based on respect for their human dignity, which forms the basis for the protection of digital heritage and information about them. Therefore, applying the right to be forgotten in the context of human dignity implies broader protection not only for the individual during his or her lifetime but also for the integrity of that person after he or she has left this world. This requires an ethical approach to handling digital heritage based on respect for the inviolability of the person and his or her dignity after death.

The European Court of Human Rights (ECtHR) has established an important legal precedent, affirming that private life is not limited to physical space but includes many important aspects of the human person. According to the ECtHR, private life includes a person's physical and social identity, personal autonomy, personal development, and the ability to establish and maintain relationships with other people and the world around them. This means that the ECtHR has a broad understanding of private life, including elements related to identity, personal development and social relationships. [142]. The European Convention on Human Rights (ECHR) emphasises the positive aspects of respecting private life, particularly by including the right to develop one's personality. Within the framework of the right to be mentioned, personal identity can be understood as a continuous story of a person's life, which no longer ends with death – this is just another event in the story. Our public persona, both during and after death, is preserved in speech, memory, and information stored in public media, equivalent to an autobiography. With the advent of the Internet, the human story becomes continuous, expanding the right to protect the digital personality after death, including the application of the right to be forgotten, which in this case becomes a tool for protecting human dignity.

The Internet allows us to tell and preserve our stories and limits the right to be forgotten. With the democratisation of data collection methods, almost everyone can collect information about others, profile them, and make frequent predictions using algorithms, thus shaping a person's future story. In addition, the data controller already has more information about an average person than the person himself, and later may be in a better position to write a story about the individual than they are themselves because the individual will never have access to some of their data. The ability to participate in the story and identity formation is undermined. Furthermore, algorithmically generated digital identities create a partial and distorted image of a person, and using digital data to create an image of a deceased person can, therefore, lead to distortions of that person's identity, image, and memories. Therefore, protecting the digital identity of social media users from distorted information remains relevant even after the end of life. The existence of digital humans and digital lives implies the role of an extension of the legal status of personality and the need for more comprehensive mechanisms to protect personality in the digital world. Creating or choosing content for one's digital identity implies providing individuals with legal tools to protect their choices fully. Implementing personal data rights after death, including the right to be forgotten, is an answer to the legal questions that

[142]Cases 30562/04 - 30566/04 S. and Marper v. the United Kingdom.

arise in the context of new technologies regarding the fate of digital assets after the data subject's death. The right to be forgotten serves as an essential counterweight to digital memory. Because now everyone can intervene in the future with their digital data. In general, we are talking about a transition to a new control over the use of data, which is a more active and less passive attitude towards data protection in the digital world. Maintaining a way of remembering and constantly accumulating information can violate the person's reputation, dignity, and inviolability after death.

REFERENCES

[1] Alessandro Mantelero (2013), The EU Proposal for a General Data Protection Regulation and the Roots of the " Right to Be Forgotten ", Computer Law and Security Review, p. 229.

[2] Aurelia Tamò Larrieux and Damian George (2014), " Oblivion, Erasure and Forgetting in the Digital Age", Journal of Intellectual Property , Information Technology and E-Commerce Law, page 74.

[3] Arvind Narayanan and Vitaly Shmatikov (2010), Myths and Fallacies of "Personally Identifiable Information" , Communications of the ACM , p. 24.

[4] Bart Custers Bart and Helena Ursic (2016), Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection, International Data Privacy Law, page 10.

[5] Bart Custers (2016), Click Here to Consent Forever: Expiry Dates for Informed Consent, Big Data & Society, page 12.

[6] Bo Zhao (2016), Posthumous Defamation and Posthumous Privacy Cases in the Digital Age, Savannah Law Review, page 15.

[7] Bert-Jaap Koops (2013), Forgetting Footprints, Shunning Shadows : A Critical Analysis of the "Right to Be Forgotten" in the Big Data practice, SCRIPTed, page 230.

[8] Cécile de Terwangne (2013), The right to be forgotten and the Informational Autonomy in the Digital

[9] Environment, Publication office of the EU, page 25.

[10] Christopher Kuner (2015), The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines, http://eprints.lse.ac.uk/61584/

[11] Clare Sullivan (2009), Digital Identity – the Legal Person? , Computer Law and Security Review, page 54.

[12] Clare Linda Sullivan (2008), Privacy or Identity? , International Journal of Intellectual Property Management, page 102.

[13] Daniel J. Solove (2004), The Digital Person: Technology and Privacy in the Information Age, New York University Press, page 96.

[14] Dan Jerker B. Svantesson (2015), Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation, International Data Privacy Law, page 23.

[15] Daniel Sperling (2008), Posthumous Interests, Cambridge University Press, page 121.

[16] Douwe Korff (2010), New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, European Commission DG Justice, Freedom and Security Report, https://ssrn.com/abstract=1638949

[17] Elad Oreg (2018), Right to Information Identity, John Marshall Journal of Computer & Information Law, page 39.

[18] European Commission (2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[19] European Commission, Factsheet on the "Right to Be Forgotten" ruling, http://europa.eu/rapid/press-release_MEMO-17-1441_en.pdf .

[20] Elena Esposito (2017), Algorithmic Memory and the Right to Be Forgotten on the Web, Big Data & Society, page 36.

[21] Evan Carroll and John Romano (2010), " Your digital afterlife: When Facebook, Flickr and Twitter are your estate, What is your legacy? ", New Riders Pub, page 98.

[22] Egoyibo Lorrita Okoro (2018), Death and Personal Data in the Age of Social Media, Tilburg University, LLM Law and Technology, page 48.

[23] Finn Brunton and Helen Fay Nissenbaum (2016), Obfuscation: A User's Guide for Privacy and Protest, MIT Press, page 15.

[24] Finn Brunton and Helen Fay Nissenbaum (2016), Obfuscation: A User's Guide for Privacy and Protest, MIT Press, page 15.

[25] Jennifer Daskal (2019), Speech across borders, Virginia Law Review, page 66. Jennifer Daskal (2019), Speech across borders, Virginia Law Review, page 66.

[26] John Perry Barlow (1996), A Declaration of the Independence of Cyberspace,

[27] https://www.eff.org/cyberspace-independence

[28] FTC (2014), Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False,

[29] https://www.ftc.gov/news-events/news/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were-false

[30] Jeffrey Rosen (2010), The Web Means the End of Forgetting, New York Times Magazine,

[31] http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all

[32] Jill Marshall (2008), Personal Freedom through Human Rights Law?: Autonomy, Identity and Integrity

[33] Joel Feinberg (1989), The moral limits of the criminal law - Self-harm, Oxford University Press, page 448.

[34] Kirsten Rabe Smolensky (2009), Rights of the dead, Hofstra Law Review, page 102.

[35] Luciano Floridi (2009), "The Information Society and Its Philosophy: Introduction to the Special Issue on The Philosophy of Information, Its Nature, and Future Developments", The Information Society, page 153.

[36] Lusine Vardanyan et al. (2022), Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity, TalTech Journal of European Studies, page 159.

[37] Mary Samonte (2020), Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law, https://www.europeanpapers.eu/en/system/files/pdf_version/EP_EF_2020_I_003_Mary_Samonte_00332.pdf

[38] Maja Ovčak Kos (2019), The right to be forgotten and the media, Lexonomica, page 195.

[39] Michèle Finck and Frank Pallas (2019), They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR, International Data Privacy Law, page 36.

[40] Norberto Nuno Gomes de Andrade (2012), "Oblivion: The Right to Be Different from Oneself - Reproposing the Right to Be Forgotten", Revista de Internet, Derecho y Política, page 122.

[41] Under the European Convention on Human Rights, Boston: Martinus Nijhoff Publishers, page 93.

[42] G comes D e A trade and Norberto Nuno (2012), The right to personal identity in the information age: a reappraisal of a lost right, Florence: European University Institute, page 12.

[43] Gianclaudio Malgieri (2018), Data Protection and Privacy: The Internet of Bodies, Hart Publishing, page 100.

[44] Meg Leta Jones and Jef Ausloos (2013), The Right to Be Forgotten Across the Pond. Journal of Information Policy, page 23.

[45] Michael L Rustad and Sanna Kulevska (2015), Reconceptualising the Right to Be Forgotten to Enable Transatlantic Data Flow, Harvard Journal of Law & Technology, page 383.

[46] Monika Zalnieriute (2020), Google LLC v. Commission nationale de l'informatique et des libertés (CNIL). American Journal of International Law, page 87.

[47] Nadezhda Purtova (2017), The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, page 40 .

[48] Norberto Nuno Gomes de Andrade (2012), Oblivion: The Right to Be Different from Oneself - Repurposing the Right to Be Forgotten , Revista de Internet, Derecho y Política , page 57.

[49] Ondřej Pavelek and Drahomira Zajickova (2019), Personal Data Protection in the Decision-Making of the CJEU Before and After the Lisbon Treaty, TalTech Journal of European Studies, page 167.

[50] OkCupid Terms and Conditions, https://okcupid-app.zendesk.com/hc/en-us/articles/23941864418203-Terms-Conditions

[51] Paul A. Bernal (2012), The Right to Online Identity https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143138

[52] Paul De Hert (2007), A right to identity to face the Internet of Things,

[53] https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf

[54] Paul Alexander Bernal (2011), A Right to Delete?, European Journal of Law and Technology, page 5.

[55] Paul M. Schwartz and Daniel J. Solove (2011), The PII Problem: Privacy and a New Concept of Personal

[56] Identifiable Information, New York University Law Review, page 50.

[57] Pam Cowburn (2019), Google win in right to be forgotten case is victory for global freedom of expression

[58] https://www.article19.org/resources/google-win-in-right-to-be-forgotten-case-is-victory-for-global-freedom-of-

expression/#:~:text=The%20CJEU%20followed%20our%20recommendations,for%20global%20freedom%20of%20expression .

[59] Paul M. Schwartz and Daniel J. Solove (2011), The PII Problem: Privacy and a New Concept of Personal

[60] Identifiable Information , New York University Law Review, page 50.

[61] Paul De Hert (2007), A Right to Identity to Face the Internet of Things, https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf

[62] Priyanshi Dixit (2019) . Will The Internet Remember You Forever? Right To Be Forgotten And Its Territorial Limits, https://www.iiprd.com/will-the-internet-remember-you-forever-right-to-be-forgotten-and-its-territorial-limits/

[63] Roger Clarke (1995), The Digital Persona and Its Application to Data Surveillance, The Information Society, page 72;

[64] Rolf H. Weber (2011), The Right to Be Forgotten: More Than a Pandora's Box?, JIPITEC, page 120

[65] Richard Hill (2016), "Internet Governance, Multi-Stakeholder Models, and the IANA Transition: Shining Example or Dark Side?", Journal of Cyber Policy, page 176.

[66] Viviane Reding, Your data, your rights: Safeguarding your privacy in a connected world ,

[67] http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm

[68] Voss G and Castets-Renard C (2016), Proposal for an International Taxonomy on the Various Forms of the "Right To Be Forgotten": A Study on the Convergence of Norms, Colorado Technology Law Journal, page 290.

[69] Viktor Mayer-Schönberger (2011), Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, page 171.

[70] Yann Padova (2019), Is the right to be forgotten a universal, regional, or "glocal" right?, International Data Privacy Law, page 45.