

THE RIGHT TO BE FORGOTTEN*

Prof. Dr. Murat Volkan Dölger* & Gülçin Gümüş*

ABSTRACT

With the advancement of technology day by day, societies continue to evolve. In this evolution process, the internet is an indispensable part of our daily lives with its social networking sites. The size of online sharing and the development of information technologies that allow access to and storage of a large number of data have led to the demand for the deletion and prevention of the dissemination of data that individuals do not want to be known by others, or in other words, the “right to be forgotten”. The right to be forgotten, which came to the agenda with the Google decision of the Court of Justice of the European Union in 2014, has been the subject of many current national and international regulations and court decisions. The right to be forgotten has gained legal status as a right under the name of “right to erasure” for the first time with the European Union General Data Protection Regulation, which entered into force on 25 May 2018. Although the right to be forgotten has not yet found a place in a legal regulation in Turkey, it is seen that some steps have been taken by the Personal Data Protection Board. This study aims to draw the framework of the right to be forgotten as a whole at the current stage.

Keywords: *The right to be forgotten, the right to erasure, personal data, personal data protection law, European Union General Data Protection Regulation.*

* This article is the English translation of our paper titled “The Right to Be Forgotten,” published in the book *Prof. Dr. Yedigir İzmirlı’ye Armağan*, Savaş Publishing, Ankara, 2024, pp. 1019–1141.

* İstanbul Aydın University Faculty of Law, Criminal Law and Criminal Procedure Law Department. muratdulger@aydin.edu.tr. <https://orcid.org/0000-0003-4034-5436>.

* İstanbul Aydın University. Graduate Student in Information Technology Law, gulcin.gumus@dulger.av.tr. <https://orcid.org/0000-0003-0047-8293>.

INTRODUCTION

Jean Valjean is a convict sentenced to hard labour; he was convicted of theft, and although he was told “you are now free” after serving his sentence, he was never truly liberated. After completing his sentence, Valjean tries to reintegrate into society but fails. Wherever he goes seeking shelter and food, he is rejected; no innkeeper wants to take him in, and every door he knocks on is slammed in his face because he is a former convict. Consequently, he transforms into an individual filled with hatred toward people, society, and life itself. For Valjean, completing his sentence does not mean freedom; although he has served and finished his punishment, his past will forever haunt him.¹

This situation raises the following questions:

1. Is Jean Valjean justified in wanting his past to be forgotten?
2. On the other hand, isn't the crime he committed also a part of history?
3. Don't the innkeepers and society have the right to know about it?
4. Is this information something that should be presented as news to the public?
5. How should a balance be struck between these competing rights?
6. If Jean Valjean's interests are prioritized, is it truly possible for his past to be forgotten?

As a being who is by nature free and constantly evolving, since his existence, man has sought the secrets to a happy² and free³ life. Undoubtedly, to achieve this, he needs a life worthy of human dignity. The most fundamental

¹ **Victor Hugo**, Sefiller, Çev. Volkan Yalçıntoklu, 8. Baskı, Türkiye İş Bankası Yayınları, İstanbul, 2019.

² The renowned philosopher and scientist Al-Farabi regarded happiness as the purpose of existence. According to him, human beings came into existence in order to be happy and act solely with the aim of achieving happiness. Indeed, the ultimate goal of all life is happiness, and a person lives in pursuit of it. Similarly, for Aristotle, happiness has always been the most valuable and fundamental goal of human life. For more detailed information, see. **Nurefşan Bulut Uslu**, Farabi ve Aristoteles'te Mutluluk Ahlakı, Kırıkkale Üniversitesi Sosyal Bilimler Dergisi, V. 8, I. 2, Haziran 2018, 469-480. See also. **Mehmet Kasım Özgen**, Mutluluk Problemi, Artus Yayınları, İstanbul, 2017.

³ According to Jean Paul Sartre, one of the leading representatives of existentialist philosophy, freedom has no foundation; rather, it is the very essence of everything. Sartre considers freedom as the fundamental condition of human existence. According to him, existence is only possible through freedom. Similarly, Nikolai Berdyaev also associated freedom with the very fabric of human existence. For more detailed information, see. **Kasım Müminov**, Nikolay Berdyayev ve Sartre Felsefesinde Kişilik ve Özgürlük Problemi, Dini Araştırmalar, Ocak – Haziran 2016, V. 19, I. 48, s. 9-24.

requirement for such a life is that a person must be equipped with the rights and freedoms that he should possess simply by virtue of being human.

The concept of human rights seeks to define the fundamental rights and freedoms that a person must possess, based on the principle that every individual should live in a manner befitting human dignity and be able to develop his or her physical and moral integrity throughout life.⁴ While the most prominent reflections of human rights law are seen in fundamental rights such as the right to life, the right to health, and the right not to be subjected to torture, the changing times and advancing technology have created a need for new rights to protect individuals.⁵ Indeed, human rights, whose boundaries were defined according to the conditions of the time when they were first established and regulated, have begun to fall short in sufficiently protecting the individual.

In this context, the greatest need has emerged with the increasing transparency of individuals due to developing technology and the progressive narrowing of the sphere of privacy. Initially, protecting only information related to private life was considered sufficient; however, over time, it became necessary to protect all kinds of data belonging to individuals. Thus, although referred to by different names such as the right to privacy, respect for private and family life, and protection of private life, the right to privacy has been recognized. In line with this, and independently of it, the right to the protection of personal data has been established, based on the principle that not only private life but also any data that helps define a person must be protected.

The right to be forgotten was initially regarded as a derivative of the right to the protection of personal data.⁶ Later, debates arose as to whether the right to be forgotten could exist independently as a standalone right, separate from the right to personal data protection. The right to be forgotten, which aims at the erasure of personal data, particularly from digital environments, has become one of the most curious and intriguing rights to emerge alongside the growing awareness of personal data protection. This right represents one of the latest discussions introduced by information technologies into the field of law and

⁴ According to the UN Vienna Declaration and Programme of Action, all human rights derive from the inherent dignity and self-worth of the human being, and the subject of human rights is once again the human being; see. Vienna Declaration and Programme of Action, 1, <https://www.ohchr.org/en/professionalinterest/pages/vienna.aspx>.

⁵ **Jack Donnelly**, *Universal Human Rights In Theory and Practice*, 3. Ed., Cornell University Press, Ithaca and London, 2013, 98.

⁶ “The right to be forgotten has always been recognized as part of the right to privacy, as it stems from the principles outlined in relation to privacy.” See. **Franz Werro**, “The Right to Be Forgotten: The General Report—Congress of the International Society of Comparative Law”, *The Right To Be Forgotten A Comparative Study of the Emergent Right’s Evolution and Application in Europe, the Americas, and Asia*, Ed. Franz Werro, Springer, Charm, 2020, 10.

reflects the need for individuals to be protected from prolonged remembrance by third parties through their personal data due to information technologies.

The subject of this study is to comprehensively examine the right to be forgotten, from its emergence to its present state. In our work, we will first identify the foundations of this right by addressing its emergence through international judicial decisions and its subsequent incorporation into international legal regulations. Then, we will try to reveal its current state both internationally, through legal regulations and court decisions, and within Turkey through the decisions of the Court of Cassation (Yargıtay) and the regulations of the Personal Data Protection Board. Within this scope, we will attempt to determine the place and significance of the right to be forgotten within the broader frameworks of human rights and the right to the protection of personal data. Thus, the foundation of this study can be summarized as follows:

“What does the right to be forgotten mean, where did it suddenly come from, what is its current state, and where is it heading?”

In this way, we aim to explain not only the legal position and regulatory framework of this right but also its philosophical foundations, thereby enabling a comprehensive understanding of the essence of the right to be forgotten.

I. The Emergence and Development of the Right to Be Forgotten

Just like the universe, the world, and life itself, human beings are also in a constant state of motion and change. As the famous philosopher *Heraclitus* said, *“You cannot step into the same river twice, for neither the river nor the person remains the same. The only constant is change itself.”* Indeed, this is one of the greatest paradoxes of the theory of sanctions, which constitutes an important part of criminal law. A person who entered prison twenty years ago for committing a serious crime is not the same person who emerges twenty years later. This is true for both the physiological and psychological aspects of the individual. Therefore, people do not want to be constantly associated with their past — especially with its negative aspects. For this reason, forgetting is not merely a right but an indispensable need for human beings. As *Friedrich Nietzsche* aptly expressed, *“Living without forgetting is impossible.”*⁷

The right to be forgotten is, in general, a new concept that enables individuals to exercise control over their personal data by requesting the removal of any information about themselves available in various environments. This right was initially recognized by the Court of Justice of the European Union⁸ and

⁷ **Friedrich Nietzsche**, Hayat Dedğin Nedir Ki?, Çev. Erkan Aslan, Aylak Adam, İstanbul, 2015.

⁸ National Civil Appeals Chamber, *Da Cunha v. Yahoo and Google*, 10 February 2010. An Argentine actress and singer, *Da Cunha*, claimed that her photographs were associated with pornographic

by certain judges in Argentina and was later supported by data protection authorities in many European countries.

The origin of this right is based on the principle that it may lead to harmful consequences if information that can identify individuals remains accessible to third parties even after many years have passed.

The ability to store data for extended periods has largely been made possible through digital systems and technological tools; therefore, the field of information technology occupies a significant place both as the cause and the consequence of this right. Today's technology enables the storage, copying, reproduction, and processing of large amounts of data.⁹ On the other hand, the use of social media platforms —most of which consist of data-sharing sites— encourages individuals to share rather than to protect their privacy and confidentiality. Especially with the increasing number of internet users, and with the emergence of the Internet of Things as a hyper-network connecting works, writings, and concepts, a massive amount of data —measurable in zettabytes or petabytes¹⁰— is produced and shared on the internet every day.¹¹ It should also be noted that a large proportion of these shared data consist of personal data. Furthermore, it must be considered that these personal data are now increasingly being used by advanced artificial intelligence software for training, data processing, and data reproduction, even if the data were initially forgotten and buried somewhere on the internet.

Therefore, the concrete cases subject to the right to be forgotten largely stem from events occurring in digital environments. However, as will be

websites on Google and Yahoo, causing damage to her career and personal beliefs, and requested the removal of these images. Judge *Virginia Simari* approached the dispute within the framework of the right to freedom of expression and the individual's right to control their own image. According to *Simari*, the right to control one's own image is among the rights of personality. *Simari* referred to an analysis by law professor *Julio César Rivera*, who argued that the right to control one's personal data also includes the right to prevent others from using one's image. Based on this, Judge *Simari* discussed the topics of updating information and deleting outdated information, offering important insights into the foundations of the right to be forgotten. For detailed information, see. Edward L. Carter, Argentina's Right to be Forgotten, <https://law.emory.edu/eilr/content/volume-27/issue-1/recent-developments/argentinas-right-to-be-forgotten.html>.

⁹ Today, there is a great diversification both in the number of digital and traditional documents produced and in the technological tools used for their production and storage. There has been an explosion in the flow of documents and information that need to be collected, preserved, and disseminated. Indeed, companies are producing information at a rate estimated to be thousands of terabytes daily. Big data coming from various mobile technologies, social media, online transactions, internet-connected objects, and their associated sensors occupies volumes measured in zettabytes or petabytes.

¹⁰ 1 petabyte (P) = 1,000,000 gigabytes (G); 1 zettabyte (Z) = 1,000,000 petabytes (P) = 1,000,000,000 gigabytes (G).

¹¹ **Abderrazak Mkadmi**, *Preservation and the Right to be Forgotten*, Archives in The Digital Age, V. 8, John Wiley & Sons, London, 2021, 113.

discussed in detail later, it should not be forgotten that data kept in physical form also falls within the scope of the right to be forgotten.

Since the deletion process involved in the right to be forgotten concerns personal data, this right primarily relies on the concepts of privacy and data protection. Nevertheless, it is also closely related to intellectual property rights, reputation rights, and the right to recognition. Furthermore, in the case of offenders, criminal law — particularly the theory of sanctions — is also relevant to the topic, as it holds that individuals who have committed crimes should not be continuously associated with or stigmatized for those crimes after serving their sentences and after a certain period has passed.¹²

However, there is also a group that approaches the right to be forgotten critically, arguing that it conflicts with freedom of expression and may lead to the repetition or erasure of history. Additionally, concerns have been raised that the right to be forgotten, affecting a large portion of society on a mass scale, could allow offenders to conceal or obscure their crimes. Thus, while the right to be forgotten is regarded by some as a necessary fundamental right, it is not universally accepted by all segments of society.

The right to be forgotten, although initially shaped by Directive 95/46/EC, essentially came to the forefront and began to be discussed following the 2014 decision of the Court of Justice of the European Union, which will be examined in detail below. Finally, with the General Data Protection Regulation (GDPR) that entered into force on May 25, 2018, it gained normative regulation (at least for EU member states). Thus, the right to be forgotten was granted legal status for the first time under the name of the “right to erasure”. Although the right to be forgotten has not yet been incorporated into any legislative regulation in Turkey, it is observed that certain steps have been taken by the Personal Data Protection Board regarding the matter. In court practices, especially concerning the application of Law No. 5651, the existence of the right to be forgotten has been recognized through case law.

It should be noted that while the GDPR introduces regulations regarding the erasure of personal data, it is not of a nature to clarify the theoretical or philosophical debates on the right to be forgotten. Therefore, although the GDPR represents an important development in establishing a legal basis for the right to be forgotten, it must be stated that it alone cannot be regarded as a complete solution to the issue.

¹² **Edward L. Carter**, “The Right To Be Forgotten”, <http://oxfordre.com/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-189>; 09.03.2019.

A. The Need for the Right to Be Forgotten

A young man, who contracted the HIV virus due to the torture and aggravated sexual assaults committed by an illegal armed organization he joined, was expelled from the organization once it was revealed that he was a carrier of the virus. Afterwards, he was prosecuted and imprisoned for the crimes he committed and served his sentence. However, when he attempted to return to normal life, he encountered great difficulties due to both his past crimes and his illness: He was ostracized by his family, was unable to find a job, could not form friendships, and realized that everyone was talking about him. Exhausted by this situation, the young man could no longer bear the burden of his past; he did not want to be remembered for his past and wished to forget it and make a fresh start. How can one escape from such a deadlock? What kind of rights category is needed for this?

The internet environment is a universal, open, and vast field of information that lacks centralized control or authority. This field of information enables any user to publish personal photographs, share comments and opinions, and even expose all their social relationships to third parties. Another individual can also publish any information—whether true or deceptive—and associate it with the user in question. As a result, due to the inherently limitless and diverse nature of internet resources, individuals find it difficult to control the dissemination of information about themselves. Moreover, there is no certainty regarding the accuracy, validity, or reliability of this information concerning the person to whom it is attributed. The real issue, however, is that such information pertains to real-world individuals: Through this, people can be harmed, their reputations damaged, and their privacy endangered!¹³

At this point, it is first necessary to refer to the striking remarks about the internet, which has led to the emergence of concepts such as big data, personal data, and the right to be forgotten: *“Information on the internet is not only accessible but also eternal.”*¹⁴

The dangers posed by the internet environment regarding personal information can be summarized as follows:

- *The Web does not forget:* Once a piece of information is published on the internet, it can be sent elsewhere and become almost impossible to

¹³ Yod-Samuel Martin/Jose M. del Alamo, “Forget About Being Forgetting: From the Right to Oblivion to the Right of Reply”, Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection, Ed. Serge Gutwirth/Ronald Leenes/Paul De Hert, Springer, Charm, 2016, 250.

¹⁴ Stefania Alessi, “Eternal Sunshine: The Right to be Forgotten in the European Union after the 2016 General Data Protection Regulation”, Emory International Law Review, V. 32, 2017, 155.

erase. Although some copies of this information can be deleted, it is always possible for it to remain elsewhere.

This danger of the internet was also highlighted by the Office of the Privacy Commissioner of Canada in its statement dated January 27, 2011, titled “Protect your personal information because the internet never forgets”.¹⁵ In this statement, the existing danger was explained as follows:

“You may not realize it, but every time you go online, you create an identity through the words you post, the images you upload, and the activities you engage in. This can become part of your reputation and may persist. Once online, it can be difficult to erase personal information. While you may be able to delete something in one place, versions or copies stored elsewhere —beyond your control— may still exist. Digital storage is cheap, and computer memory is abundant. Unlike people, the Web never forgets. Therefore, it is important to think about what you do online and to always protect your information.”

The statement also emphasized the risks posed by the persistence of information on the Web, particularly highlighting that such information could be used to embarrass individuals or damage their reputations. It was also noted that businesses could track this information without informing or obtaining consent from individuals, and that the information could be stolen and used to cause significant personal and financial harm. There is thought to be a strong public interest in restricting access to personal information on a network that never forgets.¹⁶

- *A single user cannot control the entire Web:* The lack of a central authority and the presence of independent domains such as social networking sites or blogs governed by different policies make it difficult to control existing information and to establish national legislation. Nevertheless, data subjects should have certain rights to defend themselves against data that “shapes how others perceive them” and “subjects them to public scrutiny”.¹⁷
- *The impact of information found on the Web:* On the other hand, it has been demonstrated that information found on the Web can, in some

¹⁵ https://www.priv.gc.ca/en/opc-news/news-and-announcements/2011/nr-c_110127/. 27.05.2021.

¹⁶ Office of the Privacy Commissioner of Canada, What are they saying about me? 8. https://www.priv.gc.ca/media/1810/or_201601_e.pdf. 27.05.2021.

¹⁷ **Martin/Alamo**, 250.

way, affect individuals' lives. Every day, there are studies showing that information appearing in mass communication media and escaping the control of its owners causes damage to privacy and reputation.¹⁸

In a 2013 study examining the impact of social media information on careers,¹⁹ it was first found that two-thirds of young people were not concerned that their social media use might harm their future career prospects. Nevertheless, the same study revealed that ten percent of young people had been rejected for a job because of their social media profiles and that seven out of ten recruitment officers had rejected candidates based on information found on the Web.

Indeed, Parent Teacher Association President *Catherine Davis* expressed the seriousness of the issue as follows:²⁰ *"A stupid adolescent mistake now can have significant impacts, and these records can follow them for the rest of their lives"*. If we were concerned that information about us would be remembered for a longer time, would we so freely express our views about trivial gossip matters, share our personal experiences, or make political comments, or would we censor ourselves?²¹

This situation has been explained as the chilling effect of a perfect memory altering our behaviour. In fact, *Stacy Snyder*,²² a teacher whose

¹⁸ **Martin/Alamo**, 251.

¹⁹ **Sarah Quinn**, "Facebook costing 16-34s jobs in tough economic climate", <https://ondeviceresearch.com/blog/facebook-costing-16-34s-jobs-in-tough-economic-climate>, 27.05.2021.

²⁰ Associated Press, "Naked Photos, E-Mail Get Teens in Trouble", <https://www.foxnews.com/story/naked-photos-e-mail-get-teens-in-trouble>, 27.05.2021.

²¹ **Viktor Mayer-Schönberger**, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, New Jersey, 2009, 5.

²² In the story often recounted in the context of the right to be forgotten, it is told that Stacy Snyder, a woman living in the United States who wished to become a teacher, was not allowed to teach simply because a photo showing her consuming alcohol, which she had posted on the MySpace social network in 2006, was not welcomed by the school administration. However, the actual situation is different: Snyder had studied at Conestoga Valley High School to become a teacher but was unsuccessful. She then tried to complete her credits at Millersville University in order to finish her four-year education. It was not Millersville University but her original school, Conestoga Valley High School, that would grant her the teaching diploma. It may be true that Snyder's photo on MySpace was not well-received by the school administration; however, although there was no connection between this incident and her inability to become a teacher, Snyder's lawyer filed a lawsuit against Millersville University using this as an argument. The court reviewing the case referred in its decision to reports concerning Stacy Snyder's "student-teaching" performance at Conestoga Valley High School. According to these reports, Snyder was found to be inadequate in terms of knowledge, mastery of the subject matter, grammar, conveying information, and maintaining control over students. On these grounds, the court determined that there was no connection between the MySpace photo and Snyder's failure to become a teacher and thus dismissed the case. See: Jack Herlocker, "Stacy Snyder and the Untruth That Won't Die", 22.09.2015,

job application was rejected due to information she had posted online, warned: *“Be careful about what you post online”*. Similarly, psychotherapist *Andrew Feldmar*, who was detained while crossing from Canada into the United States because of news found online about his alleged use of drugs and stimulants nearly forty years earlier—and consequently banned from entering the United States—added: *“I must warn people that their electronic footprints left on the internet can be used against them. They are not erased”*.²³

The fact that an individual’s past is never forgotten causes more problems and harm than criticisms or attacks directed at the individual’s honour or reputation. Being unable to escape one’s past and having everything from the past remembered as it can create obstacles in the individual’s process of building their future. Reminding someone of any event or phenomenon in full detail also prevents the individual from being forgiving toward themselves.²⁴

Regarding the impact of information available on the internet, American entrepreneur *J. D. Lasica* stated back in 1998—long before these issues gained widespread attention—that the consequences of the internet’s vast memory were not being adequately considered: *“Anything you post on the Internet can come back someday to haunt you. Accordingly, the traces left online remain even if we try to move away: Just like a shadow, our online life follows us wherever we go.”*²⁵

Thanks to its effect of permanence, the internet preserves bad memories, past events, writings, photos, or videos that we may later wish to deny or forget. While forgetting is a normal human activity, it contradicts what is expected from computers: In the digital age, when data is lost in a computer environment, it is considered a failure.²⁶

For individuals, the storage of data such as criminal records and credit histories means that they have no chance of being forgotten either institutionally or socially. Indeed, it is noted that new technologies have an impact on social forgetfulness. While the widespread nature of data collection practices is rightly

<https://medium.com/@jherlocker/stacy-snyder-and-the-untruth-that-won-t-die-549c2f525661>, 27.05. 2021.

²³ **Mayer-Schönberger**, 4-6.

²⁴ **Mayer-Schönberger**, 5.

²⁵ **Ângela Guimarães Pereira/Lucia Vesnić-Alujevića/Alessia Ghezzi**, “The Ethics of Forgetting and Remembering in the Digital World through the Eye of the Media”, *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*, Ed. Alessia Ghezzi/Ângela Guimarães Pereira/Lucia Vesnić-Alujević, Palgrave Macmillan, Hampshire, 2014, 11.

²⁶ **Pereira/Vesnić-Alujevića/Ghezzi**, 11.

emphasized, it is also underlined that such practices affect social memory and reduce the possibility of forgetting.²⁷

When all of this is considered together, it is possible to say that individuals need the information available in digital environments to be deleted after a certain period of time in order to be happy and free in the most fundamental areas of their lives, such as work, private, and social life.

In today's world, this right includes the individual's right to access, control, and sometimes request the deletion of personal data stored and/or processed by others. In practice, the right to be forgotten serves as a shield against media platforms, as these platforms share many types of data, including personal data, by relying on the right to inform. This right functions as a tool across the entire internet, and especially in e-commerce, enabling individuals to know, control, and potentially delete information about their own personal data.²⁸

B. The Emergence of the Right

The right to be forgotten, while being one of the newest rights to emerge with the development and awareness of personal data protection, is also one of the most widely discussed and followed. Although there are debates about whether such a right truly exists and, if so, what its scope and limits are, there is indeed a right to be forgotten that has emerged to provide a safeguard against the dangers created by the opportunities of information technologies and to meet a current need, and that has been recognized over time by judicial decisions, allowing for the erasure of individuals from memory. Accordingly, an individual whose information was obtained, collected, or processed a long time ago and who no longer has control over such data should not have to bear the burden of an event that occurred in the past today. It should be noted that the event does not necessarily have to create a negative judgment about the individual. In today's world, where the protection of personal data is paramount, the mere existence of personal data in an event over which the individual no longer has control or involvement should be sufficient to benefit from this right.

The first decision regarding the right to be forgotten concerned the responsibility of search engines. This case was brought in 2009 by Milorad (Michael) Trkulja, a 62-year-old resident of Melbourne, Australia, against Google and Yahoo. The plaintiff, Trkulja, claimed that when searching for the name of "Tony Mokbel," known as a drug lord, his own name appeared among the search results, thereby damaging his personal rights. Although Trkulja had previously been shot, it was not proven that the incident was related to drug

²⁷ **Pereira/Vesnić-Alujevića/Ghezzia**, 11, 12.

²⁸ **Werro**, 1, 2.

trafficking; nevertheless, search results on Google displayed information implying such a connection. In its defense, Google argued that it was not a content provider and that the search results were automatically pulled from news websites. The Australian court did not hold Google responsible for the content presented but stated that after the plaintiff's application to Google, the company should have delisted such content. The court found in favour of Trkulja and awarded \$208,000 in damages against Google. This decision is considered the first known ruling regarding the right to be forgotten and the right to erasure, particularly concerning search engines.²⁹ In the following period, the matter continued to come before judicial authorities and has gained increasing acceptance over time.

At the end of all these needs and developments, a new type of right has emerged in the field of personal data protection and information technology: *The right to be forgotten*.³⁰

C. The Google Decision of the Court of Justice of the European Union

1. The Importance and Impact of Internet Search Engines

The enormous societal benefit of internet search engines is an undisputed fact. Every day, people from all over the world use search engines for various activities such as shopping, research, and entertainment, as well as to communicate new ideas or stay informed about global developments. Therefore, search engines play an essential role in ensuring fundamental rights such as freedom of expression and access to information in today's information society.³¹

In addition to the benefits mentioned above, internet search engines have also raised numerous privacy concerns. In this regard, a twofold distinction can be made: (1) those relating to the users of search engine services, and (2) those relating to the subjects of the searches.³² The first group focuses on the privacy demands of individuals who use internet search engines. While searching for

²⁹ Trkulja v. Google Inc. LLC & Anor (No. 5), 2012, VSC 533, Australia Supreme Court of Victoria 12.11.2012, <http://censorshipcases.wordpress.com/2013/02/16/australia-trkulja-v-google-inc-llc-anor-no-5-2012-vsc-533-supreme-court-of-victoria12-11-2012/>, 03.06.2021.

³⁰ For this concept, see. **Meg Leta Jones**, Ctrl + Z: The Right to Be Forgotten, New York University Press, New York, 2016, 1 vd.; **Amitai Etzioni**, Privacy in a Cyber Age, Palgrave Macmillan, New York, 2015, 113-122; **Cécile de Terwangne**, "The Right to be Forgotten and Informational Autonomy in the Digital Environment", The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten, Ed. Alessia Ghezzi/Ângela Guimarães Pereira/Lucia Vesnić-Alujević, European Commission, Joint Research Centre, Palgrave Macmillan, New York, 2014, 82 – 101; **Martin Alamo**, 249 – 276.

³¹ **Brendan van Alsenoy**, Data Protection Law in the EU: Roles, Responsibilities and Liability, Intersentia, Cambridge – Antwerp – Chicago, 2019, 511.

³² **Omer Tene**, "What Google Knows: Privacy and Internet Search Engines", Utah Law Review, No. 4, 2008, 1440 vd.

information online —about personal interests, travel plans, political beliefs, sexual preferences, medical conditions, etc.— individuals reveal a great deal of personal information. In fact, the data contained in a search engine’s query logs can be even more revealing than the content of a private email or a phone conversation.³³ The second group concerns the privacy claims of the “subjects of the searches”. Internet search engines have made it relatively easy to find information about almost anyone. Using a search engine, personal data scattered across company websites, newspaper articles, social network pages, blogs, etc., which would otherwise be difficult to compile into a meaningful whole, can easily be collected, allowing the creation of a comprehensive profile about a specific individual. As a result, today people are increasingly interested in and influenced by information accessible through search engines, and they incorporate such information into various decision-making processes (e.g., recruitment, forming friendships, criminal profiling, etc.).³⁴ This task has become even easier with the use of artificial intelligence. Nowadays, even human resources companies manage recruitment processes for their clients with the support of AI software that uses such data.

Due to the impacts mentioned above, internet search engine service providers are increasingly facing requests for the removal of certain references from search results. For example, individuals may request a search engine to stop displaying one or more web pages containing personal data about them in the search results. The removal of harmful search results or references to content that invades privacy without consent can provide significant relief to the individuals affected. At the same time, such a mechanism raises a number of questions: Do search engine providers have an obligation to comply with such requests? Does it make any difference whether the content in question was lawfully published? Should a search engine provider be tasked with balancing freedom of expression and privacy? These questions lie at the very heart of the case *Google v. Spain*, decided by the Court of Justice of the European Union on May 13, 2014.³⁵

2. The Decision

The “Google Decision”³⁶ of the Court of Justice of the European Union (“CJEU”) is particularly significant in that it intensified interest and curiosity regarding the right to be forgotten and led to the recognition of this right through

³³ Tene, 1442, 1443.

³⁴ van Alsenoy, 511, 512.

³⁵ van Alsenoy, 512.

³⁶ *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD)–Mario Costeja González*, C-131/12, 13.05.2014, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>, 03.06.2021.

judicial rulings.³⁷ In the case at hand, a Spanish lawyer named *Costeja González* argued that the continued accessibility of newspaper articles mentioning the forced sale of his property to settle social security debts —dating back many years— via Google’s search engine violated Directive 95/46/EC. The Court, siding with the applicant, ruled on May 13, 2014, that based on Article 12 of the Directive concerning the right of access, personal data published under an individual’s name must be deleted once it becomes outdated or irrelevant and exceeds the original purpose for which it was collected.

The Court held that although the personal information in question had become outdated, it still involved the disclosure of the individual’s personal and financial information, and it did not find it reasonable that such information could still reach a wide audience 10 to 15 years after the original events had occurred. While these events may have caused significant moral and economic harm at the time they took place, the conditions that justified their publication were no longer present during the proceedings.

The conclusions reached by the Court in response to the questions posed, particularly those related to the right to be forgotten, can be summarized as follows:

- ***Can Google’s activities regarding data published by third parties be considered “processing of personal data” within the meaning of Article 2(b) of the Directive?***³⁸

According to Google, the activities of search engines should not be considered as data processing, since search engines relate to all information available on the internet without distinguishing between personal data and other information.³⁹

In its examination on this point, the Court relied on its previous rulings where it had recognized the uploading of personal information to a website as data processing within the scope of the Directive. Moreover, regarding the main operations, the data found, indexed, stored, and made available to users by search engines contains information relating to identified or identifiable natural persons.⁴⁰ A search engine collects such data, then records and organizes it within indexing programs, stores it on its servers, and presents it to users in the form of

³⁷ For the decision and its evaluation, see. **Armağan Ebru Bozkurt Yüksel**, *Bulut Bilişimde Kişisel Verilerin Korunması*, Yetkin, Ankara, 2016, 132 – 136.

³⁸ For example, the automatic indexing, temporary storage, and eventual provision of information published on the internet by third parties to internet users according to a certain order of preference.

³⁹ **van Alsenoy**, 521, 522.

⁴⁰ *Google Spain*, § 27.

search results.⁴¹ The Court thus concluded that the operations listed in Article 2(b) of the Directive are being carried out and that such activities could indeed be defined as data processing.

- ***Can search engines be considered data controllers under Article 2(d) of the Directive in respect of these activities?***

In its defense, Google advanced several arguments as to why it should not be considered a data controller under Article 2(d) of Directive 95/46/EC. According to Google, the main arguments for why a search engine provider should not be regarded as a “data controller” are as follows: To be considered a “data controller,” the entity in question must have a purpose for processing personal data. However, Google’s search engine indexes websites “indiscriminately” (i.e., without specifically targeting personal data). Therefore, the search engine provider cannot be considered to be acting as a “data controller” with respect to the processing of personal data contained in those websites. Instead, the publisher of such information should be considered the “data controller”. Google’s intervention in the data is, by the nature of its activities, purely “accessory” because the search engine merely makes information published by others more easily accessible. If a publisher decides, for any reason, to remove specific information from a website, that information will eventually disappear from Google’s index and will no longer appear in search results. Consequently, Google argued that the role of a search engine should be regarded as that of an “intermediary,” as described in Articles 12-14 of Directive 2000/31, or as a telecommunications service provider, as explained in Recital 47 of Directive 95/46/EC.⁴²

In response to Google’s arguments, the European Commission and various EU Member States presented substantially different counterarguments. According to these views, it is first necessary to distinguish between the processing activities of publishers (content providers) and those of search engines. Search engines carry out numerous activities (such as collecting, storing, analyzing, and ranking website content) that are entirely separate from the activities performed by publishers. The purposes and means of these activities are exclusively determined by the search engine providers themselves. Consequently, search engines should not merely be regarded as “intermediaries” but rather as providers of a “value-added service” for which they must assume their own responsibility. To reinforce this argument, it was emphasized that the harm in question primarily resulted from Google’s activities because, had the

⁴¹ Google Spain, § 28.

⁴² van Alsenoy, 522.

content not been so easily accessible via the search engine, the damage to the applicant's (*Gonzalez's*) reputation would have been significantly less severe.⁴³

The Court first emphasized that both the wording and the purpose of Article 2(d) of the Directive must be interpreted broadly in order to ensure the effective and complete protection of data subjects. In this context, it would be incorrect to exclude a search engine from the scope of the provision on the grounds that it does not have control over the personal data published on third-party web pages.⁴⁴

Moreover, according to the Court, the data processing activities of search engine operators must be regarded as separate from and additional to the processing carried out on the websites to which the search results relate.⁴⁵ As a result, the Court concluded that search engines must be considered data controllers on the grounds that they process personal data and play a decisive role in such processing.⁴⁶

While there were differing opinions as to whether search engines should be considered data controllers within the scope of such activities, the majority agreed with the Court. *Simon Hughes*, who was a Member of the United Kingdom Parliament at the time the decision was issued, argued, in parallel with the Court's ruling, that search engines should be regarded as data controllers. This is because search engines serve as a gateway to the system and often make the initial decision on whether personal data will be processed. Accordingly, being a data controller should not be limited to deciding the purpose of processing; if you are the gateway to the system, the mere fact that you act as an intermediary does not mean that you are not a data controller.⁴⁷

Similarly, *Chris Scott*,⁴⁸ a former partner at the firm Schillings, believes that Google does not merely provide information passively but also shapes search results. According to him, there is a competitive environment among search engines, and in this competition, search engines aim to help users find exactly what they are looking for in order to get ahead. Therefore, throughout

⁴³ *van Alsenoy*, 522, 523.

⁴⁴ *Google Spain*, § 34.

⁴⁵ *Google Spain*, § 35.

⁴⁶ *Google Spain*, § 41.

⁴⁷ House of Lord, European Union Committee, *EU Data Protection Law: A "Right to be Forgotten"?*, 2nd Report of Session 2014–15, The Stationery Office Limited, London, 2014, § 29.

⁴⁸ Schillings is an international reputation and privacy consultancy firm composed of experts in reputation, privacy, risk advisory, cybersecurity, and intelligence. The company operates as an Alternative Business Structure (ABS) and is regulated and authorized by the Solicitors Regulation Authority (SRA) of the United Kingdom. It provides services encompassing risk advisory, legal services, and IT security. Chris Scott is a former executive at the firm who has been promoted to partner.

this process, search engines perform a function that helps determine the way data is processed and the purposes for which it is processed by using algorithms.⁴⁹

On the other hand, there are also opposing views on this matter. For example, Professor *Neil Cameron* stated that he believes search engines are not data controllers under the Directive and that he agrees with the opinion submitted by Advocate General *Jääskinen* regarding the Court's decision.⁵⁰

In his opinion, Advocate General *Jääskinen* stated: *"In cases where the personal data processing activities of internet search engine service providers are considered to be those of a data controller, Article 6(2) of the Directive obliges them to weigh the interests of the data subjects against the interests of the data controller or the third parties on whose behalf the data processing activities are carried out. As examined by the Court in the ASNEF and FECEMD cases, whether the data in question is already available from public sources is a relevant factor in establishing this balance."*⁵¹

- ***Although the information has been lawfully published by third parties, is it still possible for such information to be subject to oblivion within the scope of Articles 12 and 14 of the Directive?***

To begin with, it is necessary to draw attention to the nature of the information at issue. This is because the data whose erasure is being requested by the data subject is accurate and has been lawfully made public. Nevertheless, the Court has stated that, in order for a data processing activity to be deemed incompatible with the Directive, it is not necessary for the data to be inaccurate. Accordingly, particular attention should be paid to whether the processing is inadequate, irrelevant, or excessive in relation to the purposes for which it is carried out.⁵² Within this context, non-compliance with the Directive may result from the fact that the information is no longer kept up to date. Therefore, even the initial processing of "accurate" data in a manner that was "lawful" at the time may, over time, become incompatible with the Directive. This is especially the case when the purposes for which the data were originally collected or processed

⁴⁹ House of Lord, The Select Committee on the European Union Home Affairs, Health and Education (Sub-Committee F) Inquiry on The Right to be Forgotten, 02.07.2014, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-sub-f-home-affairs-health-and-education-committee/the-right-to-be-forgotten/oral/11212.html>, 23.06.2020.

⁵⁰ House of Lord, Inquiry on The Right to be Forgotten, 02.07.2014.

⁵¹ Opinion of Advocate General *Jääskinen*, C-131/12, *Google Spain SL Google Inc. v. Agencia Española de Protección de Datos (AEPD)– Maria Costeja González*, 25.06.2013, § 107, <http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN>, 03.06.2021.

⁵² *Google Spain*, § 92.

no longer justify its retention, or when retention becomes inadequate, irrelevant, or —over time— “excessive” in light of the original purposes.⁵³

In light of these findings, the Court held that, where the processing carried out by the operator of a search engine results in information or links in the search results that are inadequate, irrelevant, no longer relevant, or excessive in relation to the purposes of the processing, such information and links must be removed.⁵⁴ The Court further stated that, pursuant to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the data subject may request that such information no longer be made available to the public by means of its inclusion in a search result.

By applying its findings and reasoning to the specific case, the Court identified the circumstances under which the right to be forgotten may arise and set out the constituent elements of the right:⁵⁵

- In the list of results obtained by a user conducting a search on Google based on the data subject’s name, an online archive of a daily newspaper that mentions the data subject’s name and reports on the actions taken to settle social security debts contains “information relating to the private life of the data subject” (presence of information concerning private life).
- In view of the fact that sixteen years have passed since the initial publication of this information concerning the data subject, the data subject believes that such information should no longer appear in a list of results associated with his name (passage of time).
- In the present case, when the public’s access to information concerning the data subject in the context of such a search is weighed against the applicant’s request, it appears that there are no specific reasons demonstrating an overriding public interest in accessing that information (balancing between public access and the data subject’s request).

As a result, the Court held that, in order to fulfil Articles 12 and 14 of the Directive, the search engine must delete from the list of results information relating to the data subject that has been published by third parties. Moreover, in the light of Articles 7 and 8 of the Charter of Fundamental Rights, the request for such information no longer to be included in the search results list concerns not only the economic interests of the search engine operator but also the public’s

⁵³ Google Spain, § 93.

⁵⁴ Google Spain, § 94.

⁵⁵ Google Spain, § 98.

interest in having access to that information as a result of a search relating to the data subject's name. Therefore, at this point, a balance must be struck between the interference with the data subject's fundamental rights and the overriding interests of the public.⁵⁶

To briefly evaluate this judgment delivered by the Court, the following observations should be made regarding the right to be forgotten:

- The right to be forgotten can arise only where there is a personal data processing activity and a data controller carrying out such processing.
- Information that has been lawfully and accurately disseminated may, over time, become a personal data processing activity that is incompatible with the Directive. At this point, although the personal data in the specific case had been disseminated accurately and lawfully, there is no explanation as to whether the right to be forgotten may also arise in relation to personal data that has been published inaccurately or unlawfully.
- Personal data that has become incompatible with the Directive typically refers to data which, in light of the purposes for which they were collected or processed, are no longer necessary, are insufficient, irrelevant, or have become “excessive” in the light of the passage of time and such purposes.
- In such a case, it must be acknowledged that the data subject has the right to request that their information no longer be made publicly accessible.
- The Court has established the legal basis of the right to be forgotten by stating that this right emerges from the combined interpretation of Articles 12 and 14 of the Directive and Articles 7 and 8 of the Charter of Fundamental Rights.
- Finally, a balance must be struck between the data subject's request for the information no longer to be publicly accessible and, on the other hand, the economic interest of the search engine operators as well as the public's interest in having access to such information. Thus, by demonstrating the relationship of the right to be forgotten with other rights and freedoms, the basis for the exceptions to this right—as will be examined below—has been laid. It is therefore understood that the right is not absolute.

Since 1991, *Viviane Reding*, who served for a long time as the European Union's Commissioner for Justice, welcomed the Court's decision, describing it

⁵⁶ Google Spain, § 99.

as a clear victory for the protection of Europeans' personal data. *Reding* stated: "The ruling confirms the need to bring today's data protection rules out of the digital Stone Age and into today's modern computing world." ⁵⁷

3. Google's Initiatives to Implement the Decision

Although the judgment delivered by the Court was rendered in the context of a specific case concerning *González*, who had requested the restriction of access to information about him, it is clear that its impact is far broader. The judgment applies to all data subjects, and as mentioned above, shortly after the decision, Google received a large number of applications regarding the matter. Therefore, it must be stated that the judgment imposed a significant burden even on a major company such as Google.

Within the scope of these obligations, Google initially made available a web form on 29 May 2014 through which users could submit delisting requests.⁵⁸ In addition, these requests have been publicly disclosed through the "*Google Transparency Report*."⁵⁹ According to this report, since 29 May 2014, more than six million URLs have been the subject of delisting requests.

Google has also stated, through its web form, that it removes results only from searches conducted on the basis of a data subject's name. Accordingly, for example, if it approves a request to remove an article concerning John Smith's trip to Paris, the result will no longer appear in searches for "John Smith," but may still appear in searches using different terms, such as "trip to Paris."⁶⁰

This point is significant in delineating the scope of the right to be forgotten. The Court emphasized that even though the search results in question were originally published lawfully, they may subsequently become "*inadequate, irrelevant, no longer relevant, or excessive*," and therefore unlawful, requiring removal. Google has interpreted this obligation as applying only to name-based searches.

Indeed, in the Guidelines published by the Article 29 Working Party on the matter,⁶¹ it was stated that the ruling affects only the results obtained through

⁵⁷ For the news article containing the mentioned statement, see. <https://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results>. 03.03.2024.

⁵⁸ <https://support.google.com/websearch/answer/6349986?hl=en>. 03.03.2024.

⁵⁹ <https://transparencyreport.google.com/eu-privacy/overview?hl=tr>. 03.03.2024.

⁶⁰ <https://support.google.com/transparencyreport/answer/7347822?hl=tr>. 03.03.2024.

⁶¹ Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costaja González" C - 131/12, 26.11.2014,

searches made using the individual's name and does not suggest that the page itself be deleted or removed from the index entirely. Accordingly, the page may still be accessed through the use of other search terms. Therefore, it was concluded that the right applies to all possible combinations of the individual's name, including variations and different spellings of the surname.⁶² Moreover, where it can be determined that they are linked to the individual's real identity, search terms involving "pseudonyms and nicknames" are also covered within the scope of this right.⁶³

We consider the decision to be correct in this respect within the scope of the right to be forgotten. Personal data consists of any information relating to an identified or identifiable natural person. Therefore, it is possible for personal data to be processed through the combination and processing of various types and numbers of information. However, requesting that these combinations be anticipated in advance and made unsearchable on the search engine would not only be contrary to the ordinary course of life, but would also impose an unbearable burden on search engines and constitute a technically unfeasible demand in the digital environment. Accordingly, this request must be reasonably limited. Indeed, with the decision it rendered, the Court has established such a limitation.

On the other hand, on 30 May 2014, Google announced that it had established an Advisory Council to fulfil the requirements of the decision.⁶⁴ In its statement, it was expressed that the Court's decision had placed Google in the difficult position of balancing the individual's right to be forgotten with the public's right to know, and that expert assistance had been sought to address and evaluate these matters in a detailed and accurate manner. Therefore, it can be said that Google has undertaken positive initiatives to implement the decision.

Nevertheless, independent of these initiatives by Google, the question has arisen whether it is appropriate to leave decisions on the removal of search results to search engines themselves, and this issue has become a subject of criticism. According to this view, the fact that applications will be made directly to search engines and that the evaluation and resolution of these applications will

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf. 03.06.2021.

⁶² Working Party, § 21.

⁶³ Working Party, § 13.

⁶⁴ The Advisory Board's website can be accessed via the following link: <https://archive.google.com/advisorycouncil/>. 03.06.2021.

be carried out by the search engines may hinder the genuine implementation of the decision.⁶⁵

Finally, it is necessary to consider how Google handles the requests it receives and what criteria it relies upon when assessing them. This will provide insight into the circumstances in which the right to be forgotten is applied and its scope.

Google states that, in response to the requests submitted on this matter, they seek to strike a balance between the individual's right to privacy and the public's interest in accessing information, as well as the rights of webmasters regarding the accessibility of information, which is classified as the right to disseminate information. In evaluating the requests, Google has indicated that it considers whether the search results requested to be delisted contain outdated or irrelevant information about the data subject and whether the information is of public interest.⁶⁶

Google has stated that it carries out this process within the framework of the principles established by the Article 29 Working Party and, in particular, adopts the following criteria:⁶⁷

- Is the data subject a public figure?
- Was the content requested to be removed made public at the request of the data subject?
- Could the data subject have anticipated that the content would be made publicly accessible?
- Do the data have a disproportionate impact on the data subject's personal privacy?
- Do the search results include information that puts the data subject at risk?

Google has also been criticized at this point for not being sufficiently transparent about how the balance between data subjects' privacy and the public interest is to be achieved. Another point of criticism is the absence of independent oversight in the application mechanism. In response to these criticisms, Google has admitted that it is also struggling to implement the decision and has stated that it has taken all necessary steps to fulfil it in the best possible way.⁶⁸

⁶⁵ House of Lord, European Union Committee, EU Data Protection Law: A "Right to be Forgotten"?, 2nd Report of Session 2014–15, The Stationery Office Limited, London, 2014, § 36.

⁶⁶ <https://docs.google.com/file/d/0B8syaa6SSfIT0EwRUFyOENqR3M/edit?pli=1>. 03.06.2021.

⁶⁷ Office of the Privacy Commissioner of Canada, 5.

⁶⁸ Office of the Privacy Commissioner of Canada, 5.

4. The Issue of Whether the Decision Can Be Implemented

At this point, it should first be noted that the decision applies to all search engines and therefore imposes a significant burden on the digital world. Although Google was the direct addressee of the case before the Court, the Court's ruling is binding on all search engines, both large and small. Google is the largest search engine in Europe in terms of market share and is most likely the party that will receive the majority of delisting requests. Indeed, the statistics published following the decision clearly demonstrate this.⁶⁹

As this is the first precedent-setting decision of its kind, it is clear that the same outcome will be reached in similar cases, even if it does not directly bind other search engines. Therefore, the implications of this decision and the commentary surrounding it also demonstrate an indirect binding effect on other search engines. Accordingly, search engines other than Google are, in a sense, also subject to this decision and are likewise required to take similar measures.

Regarding the question of whether the decision can be implemented, Google published the number of requests it received: Following the Court's ruling, it received twelve thousand requests across Europe within the first twenty-four hours, and approximately forty thousand within the first four days.⁷⁰ It was stated that the number of requests received within just one month meant that Google personnel had to review millions of URLs. Therefore, even by the standards of a global company like Google, this constitutes a very significant burden. Professor *Luciano Floridi*, who was appointed by Google as a member of the Advisory Council concerning the decision, responded to the question of whether it is practically possible for Google to comply with the decision by stating: *"Yes... compliance — the real issue here is not whether to comply with the decision."*⁷¹

In addition to giving rise to many new areas of debate, the decision is regarded as a symbol of the clear recognition of the right to be forgotten, as it has largely put an end to discussions over whether such a right truly exists.⁷²

⁶⁹ House of Lord, European Union Committee, EU Data Protection Law: A "Right to be Forgotten?", 2nd Report of Session 2014–15, The Stationery Office Limited, London, 2014, 14, § 31.

⁷⁰ House of Lord, EU Data Protection Law: A "Right to be Forgotten?", 14.

⁷¹ House of Lord, EU Data Protection Law: A "Right to be Forgotten?", 15.

⁷² As a result of the widespread impact of the decision, the Article 29 Working Party carried out a dedicated study on the matter and published a guideline on how the decision should be interpreted. The Court expressed the view that, in light of the potential seriousness of the impact of this process on the fundamental rights of privacy and data protection, the rights of the data subject should, as a general rule, override the economic interests of the search engine and the interest of internet users in accessing personal data through the search engine. However, a balance must be struck between the relevant rights and interests, and the outcome should depend on the nature and sensitivity of the processed data as well as the public's interest in accessing this particular information. For instance, in cases involving individuals who play a significant role in public life, it is clear that public interest will

Indeed, following the decision, there has been a significant increase in the number of applications submitted on the matter, and courts have begun to recognise individuals' right to be forgotten.

II. The Nature and Scope of The Right to Be Forgotten

A. Definition

As a newly emerging category of rights, the right to be forgotten does not yet have a well-established definition in either academic literature or international legal instruments. Moreover, the number of studies specifically addressing the issue is quite limited, and the legal regulations that recognize this right have not yet reached a level sufficient to meet the practical needs. This is not only due to the novelty of the right itself, but also to its close connection with the field of information technology law. The dynamic and complex nature of information technology law renders it a constantly evolving field that is, in many respects, open to debate.⁷³

This applies to every branch of law, but it is particularly striking in the field of information technology law. While many legal rules need to be updated as society evolves and develops, the legal rules in the field of IT law are dependent on technological advancement. However, technological progress occurs at a much faster pace than societal change. Indeed, technology has reached a point where it shapes society itself; the entire world — countries and societies alike — is progressing in line with technological developments. As a result, the legal norms governing IT law require a much faster rate of evolution. This, in turn, makes it more difficult to define and determine the scope of concepts associated with information technology law.

The right to be forgotten, in its broadest sense, refers to an individual's request to be forgotten by restricting access to their personal data.⁷⁴ The individual does not wish information that is accessible about them to be retrieved

have considerable influence on determining this balance. Accordingly, the Guideline provides an interpretation of the ruling and explains how it should be understood. In doing so, it aims to identify the criteria that data protection authorities and data controllers should consider when evaluating relevant applications. See. Article 29 Data Protection Working Party, Guidelines on The Implementation of The Court of Justice of The European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" S-131/12, 26.11.2014, 14/EN, WP 225.

⁷³ In this context, it should be noted that the right to be forgotten is not limited solely to digital data. Although digital technology has largely brought questions related to such rights to the forefront, non-digital data are also included within the scope of this right. **Mkadmí**, 151.

⁷⁴ However, there are also narrower and simpler definitions of this concept; for example: "The right to be forgotten essentially consists of being able to remove from the web certain information about past actions that are unwanted and/or could harm or injure an individual. It can also be implemented by removing one or more web pages from search engines based on a person's first and last name (removal of pages from search engines). In the first case, we refer to the right to erasure, and in the second case, to the right to de-referencing." **Mkadmí**, 150.

or disseminated, for any reason, and considers such dissemination contrary to their interests. Whether the information is accurate or up to date will be addressed below under the constituent elements of the right. However, before delving into these detailed explanations, the following questions must never be overlooked and should always be kept in mind:

- What is it that we are protecting through the right to be forgotten?
- Whom are we protecting through this right?
- What are we protecting individuals against through this right?
- Against whom are we protecting individuals through this right?⁷⁵

In Directive 95/46/EC and the GDPR, the right to be forgotten is addressed within the scope of the right to erasure and is not defined directly. Accordingly, where the data subject withdraws their explicit consent to the processing of personal data, or where the legitimate purposes for which the personal data were processed no longer exist and no other purpose remains, such data must be erased. Additionally, the right to be forgotten has been explained to require, in cases where the personal data subject to erasure have been made public, that all reasonable steps be taken by the data controller to inform all processors responsible for the dissemination of the data of the request, thereby ensuring that all copies of the data are erased.⁷⁶

From the perspective of Turkish law, the most comprehensive definition on the subject was provided by the Court of Cassation General Assembly in its decision dated 17 June 2015, as follows: “*The right to be forgotten is defined as the right to request the deletion and prevention of dissemination of personal data that one does not wish others to know — such as negative events experienced in the past that are stored in digital memory — after a certain period of time, provided that there is no overriding public interest.*”

In light of the foregoing, the right to be forgotten is a newly recognized right that enables individuals to request the removal of any information concerning them, whether in physical or digital form, thereby ensuring that they are no longer associated with such personal data and allowing them to exercise control over their personal information.

B. Methods of Exercising the Right

The right to be forgotten may generally be exercised through four distinct methods: Delisting, anonymization, erasure, and restriction of access. The

⁷⁵ Mkadmi, 150.

⁷⁶ For the relevant explanation, see. <https://gdpr-info.eu/issues/right-to-be-forgotten/>, 23.05.2020.

question that arises at this point is how realistic these methods are and to what extent they effectively ensure the exercise of this right.⁷⁷

While memorising and recalling information requires a conscious effort for humans, forgetting is a natural and unconscious process. In contrast, unlike the human brain, no scientific advancement has yet been developed to replicate this mechanism in computers. On the contrary, in the digital world, forgetting constitutes a technical challenge and requires deliberate effort.⁷⁸

The right to be forgotten cannot be viewed solely as a right to erase information or prevent its dissemination. In a rapidly evolving technological world, this right must be understood and addressed in a multifaceted manner. At its core, the right to be forgotten is an expanding right, and it may also be defined as the right of individuals to exert greater control over their personal data. Just as it was originally conceived in the pre-internet era, in the post-internet era as well, the legitimacy of this right derives from the recognition of personal freedom, human dignity, and the right to self-determination. Rooted primarily in the value of privacy, the right to be forgotten manifests itself as an individual's right to control their personal information—even after it has been disclosed—and to reclaim or erase it. In this regard, *Whitman* aptly frames the concept by stating that “*the right to privacy appears as a right to informational self-determination, that is, the right of the individual to control the kinds of information disclosed about them.*”⁷⁹ However, this approach must not be understood to imply that individuals are entitled to control information that serves the public interest.⁸⁰

C. Elements

Nevertheless, the mere existence of an ordinary person and ordinary information about that person is not sufficient for the right to be forgotten to come into play. For the right to be applicable and enforceable, the context in which the information about the individual is made available must exhibit certain characteristics. Understanding these characteristics depends on identifying the elements of the right to be forgotten. In this way, the precise scope and meaning of the right can be better understood.

As mentioned above, given that the right to be forgotten does not yet rest on firmly established foundations, it does not possess clear, specific, and

⁷⁷ MKADMI, 156, 157.

⁷⁸ MKADMI, 157.

⁷⁹ **James Q. Whitman**, “The Two Western Cultures of Privacy: Dignity versus Liberty”, *Yale Law Journal*, Vol. 113, No. 6, 2004, 1186, 1210.

⁸⁰ **Werro**, s. 18. See also. **Robert C. Post**, “Data Privacy and Dignitary Privacy: Google Spain, The Right to be Forgotten, and the Construction of the Public Sphere”, *Duke Law Journal*, V. 67, 2018, 1051.

well-defined elements. Nonetheless, its constituent elements may be broadly summarized as follows:

*1. Element of Publicly Disclosed Personal Data*⁸¹

The subject matter of an individual's right to be forgotten consists of their publicly disclosed personal data. More precisely, the individual's request to restrict access under the right to be forgotten pertains to personal data that is publicly available. Through the exercise of this right, the individual seeks to prevent access to such personal data. Accordingly, the individual holds the right and authority to request the erasure of information that is personally identifiable. This is because personal data refers to any information that identifies or makes it possible to identify a natural person. At this point, although the protection of personal data is closely related to the right to be forgotten, we shall refrain from diverging from the main topic and limit ourselves to providing only the definition of personal data, without delving into the details of data protection law.⁸² In any case, the concept of personal data will be frequently referred to throughout this study, and the right to the protection of personal data will be addressed in connection with other rights related to the right to be forgotten.

While the subject matter of an individual's right to be forgotten is indeed their personal data, it must be emphasized that such personal data must be publicly available. Furthermore, the presence of the criteria set out below must also be taken into consideration in the assessment.

a. The Circumstances at the Time the Personal Data Was First Made Public and Disseminated

Whether the personal data that an individual may invoke under the right to be forgotten was initially disseminated lawfully is significant in terms of the element of personal data. Lawful dissemination refers either to the existence of one of the legal grounds for data processing or, in the absence of any such ground, the presence of the data subject's explicit consent.

For instance, when examining the concrete cases most frequently associated with the right to be forgotten, reference can be made to the situation

⁸¹ This element has also been referred to as the "information element" in national sources on the subject. See. **Eren Sözüer**, *Unutulma Hakkı: İnsan Hakları Hukuku Perspektifinden Bir İnceleme*, On İki Levha Yayıncılık, Ankara, 2017, 43. However, since the exercise of the right to be forgotten requires the existence of information that can be associated with the individual—i.e., personal data—I preferred to treat this element as the personal data element. Although the terms "information" and "data" will be used interchangeably throughout the study, I find it more appropriate to use the term "data" when referring to the elements of the right. For the difference between the concepts of information and data, see. **Murat Volkan Dülger**, *Kişisel Verilerin Korunması Hukuku*, 3. Baskı, Hukuk Akademisi, İstanbul, 2019, 153.

⁸² For detailed information on the concept of personal data, see. **Dülger**, *Kişisel Verilerin Korunması Hukuku*, (3), 151-176.

of a person who has committed a crime. The reporting of such an individual on television channels or internet sites undoubtedly constitutes an interference with their right to privacy and the protection of their personal data. However, when the rights in question — the individual's right to privacy and data protection — are weighed against freedom of expression, freedom of the press, and the public's right to access information, the publication of such news is considered to serve a higher interest, as the public has a right to be informed. Indeed, it must not be forgotten that even fundamental rights and freedoms such as the right to privacy and the protection of personal data may be restricted in accordance with the principle of proportionality, provided that the necessary conditions are met.

In the absence of any legitimate purpose for the processing of personal data, the explicit consent of the data subject is required for the data to be processed. It should be noted that, in a given case, where one of the legal grounds for the processing of personal data exists, obtaining explicit consent would be unlawful. The presence of the data subject's explicit consent to the processing — in other words, the disclosure and dissemination — of their data, or the fact that the data have been made public by the individual themselves, indicates the existence of such consent. Therefore, the personal data in question would be considered lawful at the time of its initial publication. A common example of this is the data subject's posts on social networking sites. With the advancement of technology, individuals have gained the ability to publish content online. Indeed, most of the content shared today occurs in this manner.⁸³ The dissemination of personal data by an individual through a social networking site or through their own website, channel, or blog falls within this scope.

In conclusion, personal data that is made public either on the basis of one of the legal grounds for data processing or with the explicit consent of the data subject constitutes data that is lawfully disclosed at the outset.

At this point, the issue to be discussed is whether, for personal data to fall within the scope of the right to be forgotten, it must have been lawfully disclosed at the time of its initial publication, or whether both lawful and unlawful disclosures are equally subject to the right, regardless of their legality. There are differing views on this matter: According to one view, the information subject to the right to be forgotten must have been lawfully disclosed.⁸⁴ Information

⁸³ A study conducted in 2017 reveals the extraordinary scale of content shared on the Web in an extremely short period of time. According to the research, in 2017, users uploaded an average of 243,000 photos to their Facebook accounts and made 350,000 posts on Twitter every single minute. Meanwhile, the total duration of calls made by Skype users worldwide in a single minute reached two million minutes. For the graph of the mentioned study, see: <http://www.go-globe.com/blog/things-that-happen-every-60-seconds>, 23.05.2020.

⁸⁴ See. Sözüer, 43. Although the author states that the information must initially have been lawfully disclosed, and then adds that "*however, these characteristics may vary in different aspects of the right to be forgotten*," it is not entirely clear what is meant at this point.

lawfully published may later be made subject to the right to be forgotten by the data subject. Another view holds that the distinguishing feature of the right to be forgotten is that it applies not only to unlawfully disclosed data but also to data that was lawful at the time of publication. According to this perspective, the right to be forgotten is applicable to both lawfully and unlawfully disseminated data.⁸⁵ Some authors, on the other hand, do not draw such a categorical distinction; rather, by examining the cases in which the right to be forgotten has been invoked, they observe that the information in question was, in general, lawfully made public at the outset. It is also noted that the individuals requesting erasure generally do not claim that the data was made public unlawfully or that it was inaccurate. Since this generalisation is based on actual cases, we believe that an accurate assessment of the current situation has been provided.⁸⁶

In our opinion, it is not possible to draw a strict distinction whereby the right to be forgotten applies exclusively to either unlawfully or lawfully disseminated data. Nor do we consider such a distinction to be correct. Indeed, if the personal data in question was initially published unlawfully, there is nothing to prevent it from being made subject to the right to be forgotten. However, the following situation may arise where personal data was initially disclosed unlawfully, invoking the right to be forgotten may be neither necessary nor beneficial. In such cases, the violation pertains to the right to the protection of personal data — which already provides broader and more explicit protection than the right to be forgotten — and, though not always, most likely also constitutes a violation of the right to privacy. Therefore, where the unlawful disclosure of personal data is concerned, it would not be in the interest of the data subject to seek redress under the right to be forgotten. In such circumstances, it would be more reasonable to assert a violation of the right to the protection of personal data or, where the conditions are met, a breach of the right to privacy. Nevertheless, we believe that — in the absence of a clear legal provision to the contrary — a definitive exclusion of unlawfully disclosed data from the scope of the right to be forgotten should be avoided.

b. Whether the Personal Data Is Accurate or Not

Whether the personal data subject to the right to be forgotten must be accurate is another aspect of the concept of personal data that requires

⁸⁵ **Can Yavuz**, İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması: Unutulma Hakkı, Seçkin Yayıncılık, Ankara, 2016, 55, 56.

⁸⁶ **Cemile Turgut**, Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı, On İki Levha Yayıncılık, İstanbul, 2021, 239. However, the author subsequently states that in cases where the act of making information public was unlawful from the outset, the issue should be evaluated within the scope of rights such as the protection of private life or the protection of honour and dignity. From a normative perspective, we believe that the right to be forgotten should also come into play in cases involving data that has been made public unlawfully.

discussion. There is no need to debate inaccurate information that does not identify a person. However, it is controversial what should happen when the personal data, while being capable of identifying a real person, contains incorrect or incomplete information. For example, such a situation arises where an individual has been acquitted in a criminal case, yet information has been disseminated within their workplace indicating that they were convicted.

In essence, personal data that is inaccurate at the time of its initial publication is similar in nature to unlawfully disclosed personal data. In our view, it would be incorrect to draw a strict line excluding inaccurate information from the scope of the right to be forgotten. This is because, in such cases, the data subject may already benefit from broader rights under the right to the protection of personal data — such as the right to rectification or the right to have data updated — rather than relying solely on the right to be forgotten. Therefore, invoking the right to be forgotten may not serve the data subject's best interest in such instances. However, the data subject is not obliged to request the correction of inaccurate information with accurate data; they may also directly request its deletion. Nonetheless, it should be emphasised that there is no barrier to invoking the right to be forgotten in relation to inaccurate information.

c. Whether the Personal Data Must Contain a Negative Judgment

As a final point concerning the element of personal data, it should be examined whether personal data subject to the right to be forgotten must contain a negative judgment from the perspective of the data subject, even where the data were accurate and lawfully disclosed at the time of their initial publication. In other words, the data in question were lawfully published and contained information that was accurate in relation to the data subject. In such a case, must there be a negative judgment regarding the data subject in order for the right to be forgotten to arise? Or can the right be exercised regardless of whether the content is negative or positive?

By negative judgment, what is meant is the accessibility of data that may cause discomfort to the individual. For example, a newspaper article relating to a crime the person has committed, or an image shared by the individual on their own social media account that may lead to negative impressions, falls within this scope. However, the real question to be asked here is this: Must the data accessible to the public necessarily contain a negative judgment about the data subject in order for the data subject to be disturbed by it? Can the data subject not later become uncomfortable with a photograph that contains no objectively negative content, based solely on subjective reasons? This is, of course, possible. One may not wish for a photograph or video shared today to be accessible in the

future or may simply wish not to appear in the press — even in the case of a newspaper article that portrays them in a positive light.

At this point, it must be emphasised that the event in question does not necessarily have to give rise to a negative judgment about the individual. In today's context, where personal data are protected as such, the mere presence of personal data in an event that occurred long ago — over which the data subject no longer has control or oversight — should be sufficient for invoking this right. Therefore, this determination should be left to the discretion of the data subject. Indeed, the notion that only negative personal data may be subject to erasure is incompatible with the fundamental principles of data protection law. It is the data subject who decides what is positive or negative, and whether they wish to be associated with that information — regardless of whether it is favourable or unfavourable.

2. The Element of the Data Subject

Another debated aspect of the right to be forgotten is whether it is granted exclusively to natural persons or whether legal entities may also benefit from this right.

Whether the right to be forgotten can be applied to legal entities essentially depends on the approach adopted toward the nature of the right. If it is regarded as a human right, then it cannot be expected to extend to legal entities. Conversely, if it is argued that the personality of legal entities should also be protected and that damage to their reputation and dignity should be prevented, then the view may be adopted that legal entities, too, can benefit from the right to be forgotten.

Looking further back, the approach to the right to the protection of personal data — a right closely connected to the right to be forgotten — is also of significance. We should emphasise that we consider the right to the protection of personal data to be a human right.⁸⁷ The right to be forgotten shares similar principles with data protection and is also rooted in the individual's need to be forgotten as they continue their life. Therefore, in terms of its origins and theoretical foundations, we believe the right to be forgotten should be regarded as a human right and applied exclusively to natural persons. However, it must be noted that this reflects the current perspective and may vary depending on the evolving role of legal entities.

⁸⁷ **Murat Volkan Dülger**, "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Y. 5, S. 1, Bahar 2018, 77-82.

Indeed, the right to be forgotten is currently applied exclusively to natural persons. Even the application of this right to natural persons remains the subject of considerable debate, while its application to legal entities is still highly uncertain. Nonetheless, there have been various concrete cases in which legal entities have asserted claims to benefit from the right to be forgotten, and this issue is actively being discussed, particularly in European countries.

As previously noted, the position of legal entities will be addressed in greater detail below. At this point, it must be reiterated that, under the current state of the right to be forgotten, the element of the data subject requires the existence of a natural person, and there is no precedent for its application to the contrary.

3. The Temporal Element

Perhaps the most significant reason why the right to be forgotten is situated in a markedly different position from other rights is the temporal element. While the passage of time is of little relevance to other rights — and, in most cases, the exercise of the right occurs at the moment the unlawfulness or violation arises — the situation is quite different with respect to the right to be forgotten. More than that, the emergence of the right to be forgotten is, in fact, dependent on the passage of time; in other words, it is the lapse of time itself that constitutes the element of unlawfulness in the context of this right.

As previously mentioned, the absence of any unlawfulness at the time personal data is first made public and disseminated indicates either the presence of one of the legal grounds for processing or the explicit consent of the data subject. In cases involving unlawful processing, the right to the protection of personal data is already being violated, and it is therefore possible to invoke that right directly, making the exercise of the right to be forgotten unnecessary. If the data is detrimental to the data subject at the time of publication, they may invoke their rights to privacy or personal data protection to allege unlawfulness and seek redress. However, when personal data is initially published lawfully, the right to be forgotten may later come into play due to the passage of time or changing circumstances. Accordingly, the right to be forgotten typically arises from a situation that was initially lawful.

So, what changes must occur for the right to be forgotten to arise in relation to a situation that was initially lawful? At this point, the passage of time between the date the data was first published and the moment the right to be forgotten is invoked becomes relevant. During this period, the following changes may occur with respect to data that was lawfully disclosed at the outset:

- The purposes for processing the personal data no longer exist,

- The data contain insufficient, incomplete, irrelevant, or inaccurate information about the data subject,
- The data involve information that exceeds or falls outside the purposes of processing, or has been used or disseminated in a manner contrary to such purposes,
- Even when the purposes of processing are taken into account, the data include information that is excessively related to the data subject,
- The public interest in the information has diminished,
- Beyond all of these, the passage of time, changing circumstances, and the evolving nature of the individual must be taken into account.

When we consider the first possible changes, we observe a close connection with data protection law. In such cases, a personal data processing activity that was initially lawful often becomes unlawful over time and therefore falls within the scope of data protection regulations. It is precisely from this point that the close relationship between the right to be forgotten and the right to the protection of personal data arises. So much so that it has been argued that the right to be forgotten is inseparable from and should be regarded as a component of the right to personal data protection. While we do not fully share this view, we do wish to emphasise the close connection between the two rights, which cannot be separated by strict boundaries. Accordingly, although the first set of situations primarily falls within the scope of data protection law, they may also give rise to issues concerning the right to be forgotten.

However, beyond all of these, there is a distinct temporal dimension — and it is precisely in this area that the right to be forgotten most clearly comes into play. This is the point at which the right to be forgotten, although occasionally intersecting with other rights, reveals its unique character.

The importance of the temporal element is first reflected in the diminishing public interest in the information as time passes. Accordingly, a historical event should no longer be revived after a significant period has elapsed. The further back in time the information dates, the greater the likelihood that personal interests will outweigh public interests. As the individual's control over the information increases over time, the importance and relevance of that information to the public simultaneously diminish.⁸⁸

Beyond this, as noted above, life itself — and human beings — are in a constant state of movement and change. Time is one of the primary drivers of this transformation. With the passage of time, both circumstances and

⁸⁸ **Rolf H. Weber**, *The Right to be Forgotten: More Than a Pandora's Box?*, 2011, s. 121. <https://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf>. 23.05.2020.

individuals evolve. As a result of such change, an individual often no longer wishes to be associated with who they were before. While this is frequently the case following a negative experience in the past, it does not always require the occurrence of a harmful event. Change may mean that someone who once committed a wrongful act later becomes a better person and refrains from wrongdoing. Moreover, categorising individuals simply as “good” or “bad” would lead to flawed assessments.

However, it is undeniable that the right to be forgotten most frequently arises in the aftermath of a committed offence or a negative event experienced by the individual. After all, even if a person recognises that they or their circumstances have changed, they are generally less inclined to request the erasure of positive information about themselves. For instance, a businessman who went through a difficult financial period and filed for bankruptcy may be more likely to want to distance himself from that event years later, compared to another businessman who, even after a long time, would likely welcome being remembered for his successes or charitable contributions. In our opinion, there is no obstacle or drawback to the data subject invoking the right to be forgotten in such cases as well; however, it is a concrete reality in practice that this right is almost exclusively exercised in relation to negative events.

This is precisely where the relationship between criminal law and the right to be forgotten comes into play. It concerns one of the most persistent and unresolved issues in criminal law. An individual may be sentenced to a long term of imprisonment for a crime committed, but during this time, the person who is incarcerated — the convict whose sentence is being served — undergoes personal transformation. While it is generally hoped and assumed that this change will be positive and forward-looking, such transformation should not be perceived solely in that light. Nonetheless, some form of change is inevitable.

As a result, with the passage of time, individuals undergo both physical and psychological changes. Consequently, they no longer wish to be continually associated with their “former selves” or, more generally, with their past. For this reason, being forgotten is not merely a desire but an essential need in terms of the temporal element — allowing individuals to continue their lives independently of the negative events they have experienced in the past.

Indeed, *Friedrich Nietzsche* theorised this need in his work referred to as the “active forgetting thesis”. *Nietzsche* grounded the human need to forget in the notion of historicity. According to him, the greatest difference between humans and animals lies in “historicity”: Animals lack a sense of historicity and live without feeling any distinction between yesterday and today. Humans, however, possess a historical consciousness that distinguishes them from

animals, and they constantly carry the past with them. For *Nietzsche*, the only condition for being truly happy is the ability to forget.⁸⁹

Human forgetting undoubtedly depends on being forgotten. A person can only forget when they are no longer remembered or associated with their past. Therefore, among all the elements related to the right to be forgotten, we believe that the temporal element is particularly important for understanding the underlying idea and philosophy of the right itself.

At this point, the question may arise as to whether a specific period of time must pass in order to exercise the right to be forgotten. We should note that the notion of allowing the right to be exercised only after a clearly defined period has elapsed would not align with the philosophical understanding we have outlined above. Indeed, no such fixed timeframe exists. However, since individuals generally seek to invoke the right to be forgotten after a certain amount of time has passed or certain changes have occurred, it can be said that, by its very nature, the right typically presupposes the passage of time. Nonetheless, this does not imply that there must be a concrete and predefined duration.

In conclusion, at the core of the right to be forgotten lies the ability of an individual to object to the use of their personal information in different contexts after a certain amount of time has passed. Accordingly, the right to be forgotten is directly linked to the concept of informational autonomy. A piece of information relating to a person's past may not have caused them discomfort at the time it occurred; however, over time, the indexing of such information by search engines may present various concerns for the data subject — who may no longer wish to be associated with that information. In this respect, the right to be forgotten also encompasses the right of individuals to change their minds or to feel regret regarding such information. The desire of individuals to avoid the constant recall of information about themselves lies at the heart of the concept of forgetting that we previously described. Therefore, the right to be forgotten offers individuals the opportunity to regain control over personal data for which such control had been lost.

4. The Medium in Which the Data Is Contained

Finally, it is necessary to examine whether the right to be forgotten carries any specific characteristics in relation to the medium in which the personal data is contained. Must the personal data that the data subject wishes to make

⁸⁹ **Friedrich Nietzsche**, *On the Advantage and Disadvantage of History for Life*, Translated by. Peter Preuss, 15. Ed., Hackett Pub Co, Cambridge, 1980.

inaccessible be in a digital environment? Or can the right to be forgotten also be exercised with regard to personal data found in a physical medium?

At this point, we would first like to refer to the origin of this question. As previously mentioned, the right to be forgotten emerged in connection with the development of information technologies. Although the importance of forgetting has always been recognised, there was previously no need for protection of this kind, as there was no medium capable of retaining data for such extended periods as to require forgetting. However, with the advances in information technologies, it has become possible to both record vast amounts of data and store them for long durations. Therefore, although the need to forget data has always existed, the need for legal regulation and protection of this right has essentially arisen in conjunction with digital technologies. So much so that some scholars consider the right to be forgotten as a legal right specific to the field of IT law.

Accordingly, there is no doubt that the legal recognition and protection of the right to be forgotten has been made possible primarily through information technologies. Nonetheless, we do not consider it appropriate — from the perspective of the individual's need to be forgotten — to limit the right solely to data in digital form for this reason alone. It is indeed possible for data in a physical medium to also fall within the scope of the right to be forgotten. In fact, as will be explained in greater detail below, a decision by the Court of Cassation General Assembly on the matter explicitly states that “...*the right to be forgotten is not limited solely to personal data in digital media...*” thereby affirming that the right may also be applied to data stored in physical environments.

D. Purpose and Protected Interests

From a broad perspective, the logic of rights and the values they protect also supports the existence of such a right. First of all, individuals have a legitimate interest in keeping their data secure and are therefore inclined to request the deletion of data that concerns them. Beyond this concern, individuals assert such a right based on the simple belief that they ought to have it.⁹⁰

This idea aligns with research conducted in 2009 by the University of Pennsylvania on public attitudes toward behavioural advertising. According to the study, 92% of respondents believed that there should be a law requiring websites and advertising companies to delete all information about an individual upon request. While this may not be sufficient to draw definitive conclusions, it clearly indicates a situation that must be taken seriously. It demonstrates, at the very least, that the right is supported at a pragmatic level. Indeed, Google CEO

⁹⁰ **Paul Bernal**, *Internet Privacy Rights - Rights to Protect Autonomy*, Cambridge University Press, Cambridge, 2014, 178.

Eric Schmidt also acknowledged this in a statement made on 6 May 2013.⁹¹ In his view, the absence of a delete button on the internet is a significant and debatable issue, as there is a time when deletion is the right thing to do.⁹²

The values that the right to be forgotten seeks to protect may be grouped under three main categories. The first concerns society at large, the second pertains to the data subject, and finally, there is the objective of preventing data pollution through the deletion of unnecessary information.

1. The Right to Be Forgotten as a Human Right

In terms of the values it protects, the right to be forgotten should first be considered within the framework of human rights. At this point, rather than engaging in the direct debate over whether the right to be forgotten qualifies as a human right, we would like to draw attention to a different perspective. The first value protected by the right to be forgotten should be approached from a much broader standpoint than the mere assurance and protection it provides to the data subject.

In connection with the subject under examination, there is no doubt that fundamental rights and freedoms such as the right to privacy, freedom of expression, and freedom of communication are recognised as human rights. Subsequently, the right to the protection of personal data — although not yet entirely free from debate — is largely regarded as a human right as well. In order to determine whether the right to be forgotten also falls within this scope, it is necessary to consider the fundamental principles embraced by the concept of human rights.

The concept of human rights can be defined as the rights that stem from an individual's physical and spiritual existence and that one inherently possesses by virtue of being human. However, understanding human rights is not possible merely through a definitional approach. Human rights encompass a much broader and more profound ideal than simply defining a term, word, or phrase. To this end, it is necessary to consider the principles and phenomena that form the foundation of human rights and help guide our understanding of what human rights truly mean.

Human rights are fundamentally based on the protection of the material and moral integrity of the individual.⁹³ The measure by which an individual can

⁹¹ For the interview containing the relevant statement, see. <https://www.businessinsider.com/schmidt-internet-needs-a-delete-button-2013-5>, 23.05.2020.

⁹² Bernal, 178.

⁹³ Kahan Onur Arslan, "İnsan Onuru ve Koruma Tedbirleri Bağlamında Temel Bir İlke Olarak İnsan Onurunun Korunması", Türkiye Barolar Birliği Dergisi, S. 120, 2015, 156, 157.

develop their material and spiritual existence is human dignity.⁹⁴ This is because the preservation and development of one's personality require the ability to exist in a manner befitting human dignity. According to the Constitutional Court, human dignity refers to the recognition and respect for the intrinsic value that a person possesses solely by being human, regardless of their circumstances or condition. It represents a moral baseline below which any treatment would strip the individual of their very humanity.⁹⁵

This understanding — that the rights which emerge in response to the negative effects of technology on human life are fundamentally aimed at protecting human dignity — also reveals the connection between the right to be forgotten and human dignity. The spread of technological developments and the internet has led to increased exposure of private life and the narrowing of one's sphere of privacy, thereby heightening the risk of harm to human dignity. Since human dignity constitutes a non-negotiable domain that must not be placed at risk, new rights must be developed to protect it. Although the right to be forgotten has existed in various forms throughout history, it is among the rights formulated with this very aim in mind. Accordingly, it may be said that the right to be forgotten is fundamentally intended to safeguard human dignity.

This connection was first established in the judgment of the German Federal Constitutional Court dated 5 June 1973, known as the “Lebach” decision.⁹⁶ The case concerned a robbery of munitions depot belonging to the German armed forces, during which several guards were killed or seriously injured. A convicted individual who had been arrested for the incident and sentenced to six years in prison later filed a complaint after a German television channel produced a documentary about the event, frequently mentioning his name. He argued that this constituted an infringement of his personality rights and sought a ban on the broadcast of the documentary as well as compensation.

The Mainz Regional Court held that the convict was “a figure of relatively recent history” and therefore could not rely on the right to the protection of personality. The Koblenz Court of Appeal, on the other hand, accepted that the matter had to be evaluated in light of the personality rights protected under Articles 1 and 2 of the German Constitution. Nonetheless, it concluded in its judgment that, given the freedom to receive information protected under Article 5 of the Constitution and the convict's status as a historical figure, the interests of the public prevailed.

⁹⁴ **Ali Tarık Gümüş**, “Türk Anayasasında Kişinin Maddi ve Manevi Varlığını Koruma Geliştirme Hakkı”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 13, S. 2, 2005, 139.

⁹⁵ AYM, E. 1963/132, K. 1966/29.

⁹⁶ BVerfGE 35, 202, 05.06.1973.

German Federal Constitutional Court, however, adopted a more comprehensive approach. It first emphasised that Articles 1 and 2 of the German Constitution safeguard the individual's right to freely develop their personality and human dignity and protect the sphere of personal autonomy in which everyone is free to shape their private life. The Court acknowledged, even within its own case law, that not all aspects of private life are afforded absolute protection. Nonetheless, neither the state's interest in preventing and prosecuting crimes nor the public interest in general can always justify the violation of personality rights. Instead, due consideration must also be given to rights closely linked to human dignity, such as the right to free personal development and respect for personality.

The Federal Constitutional Court highlighted the clear conflict between the rights to human dignity and personal development, and the freedoms of information and the press. Resolving this conflict requires the establishment of a proper balance. According to the Court, while the freedom of expression may have a limiting effect on claims based on personality rights, any resulting harm to the individual's personality must be proportionate to the importance of the communication in terms of protecting freedom of expression in a democratic society.

At precisely this point, the Court offers an important clue regarding the right to be forgotten. According to the constitutional guarantee of personality rights, the media cannot be permitted to engage with a convicted person and their private life "indefinitely." Even a person who has committed a serious crime, attracting public outrage and widespread disapproval, remains a member of the community and, within this context, continues to retain the constitutionally protected right to the safeguarding of their personality.⁹⁷ Although a conviction handed down by a criminal court may have been published in the public interest and met with legitimate public reaction, this cannot justify the continued or repeated intrusions into the personal sphere of the offender, nor can it serve to normalise such invasions. Furthermore, the Court noted that it is not possible to set a specific time limit in terms of months or years that would apply uniformly to all cases.⁹⁸

This case is particularly significant in that it reveals the importance of the right to be forgotten in terms of human dignity and the right to develop one's material and moral existence. Moreover, it does so within the framework of the freedoms of access to information and dissemination of information. Additionally, by stating that events are part of historical memory, it also takes

⁹⁷ The court explained this using the concept of the "right to be left alone".

⁹⁸ BVerfGE 35, 202 – Lebach, Bundesverfassungsgericht (First Division) 05.06.1973.

the concept of historicity into account. Since situations in which the right to be forgotten conflicts with these concepts will be addressed separately later on, we will limit ourselves here to discussing the relevance of this case to the right to be forgotten.

Lastly, it should be emphasized that human dignity and the right to develop one's material and moral existence are matters that concern society as a whole, far beyond pointing directly to a specific individual. Therefore, we find it more appropriate to examine the values protected by the right to be forgotten from this broader perspective.

2. Forgetting the Data Subject

After the values protected by the right to be forgotten within the context of human rights, its most significant impact is undoubtedly on the data subject directly. This is because the person to whom the right is granted is the data subject, and it is also the data subject who will request to be forgotten.

If we are to transition from the concept of human dignity to the data subject, it is necessary to address the relationship between human dignity and the autonomous individual. Accordingly, one of the fundamental objectives that human dignity seeks to achieve is to create an autonomous space in which the individual can develop their material and moral existence. Within this space, the individual must have the opportunity to shape their own life and to develop themselves. In doing so, they must be able to act according to their own will, rather than in response to external influences.

In accordance with the concepts of human dignity and autonomy, an individual who is to shape their life as they wish must also have the same freedom over their personal data. Since an individual who lacks control over their own data cannot be considered autonomous, the goal of human dignity likewise cannot be attained.

It is evident that an individual who perceives their personal data as vulnerable will take this matter seriously. If individuals believe that their personal information can easily be lost or fall into the hands of potential criminals or those who may wish to use it against them, they will feel at risk: *"If data is vulnerable, then people are vulnerable; if data is under threat, then they themselves are under threat."*⁹⁹

This is precisely why the use or misuse of data can directly lead to threats against autonomy. Indeed, the feeling of threat holds great significance for

⁹⁹ Bernal, 176.

autonomy. Therefore, individuals must have greater control over their data and must also feel that they possess such control.¹⁰⁰

The nature of this threat to autonomy is seen as qualitatively different from general data protection threats. This is because, in most situations where a danger exists in data processing activities, there is at least some degree of justification on the part of the data controller for the collection and use of the data. The situation with search engines, however, is different: Search engines aim to collect data from searches, and what happens to the data or who collects the data cannot be foreseen by the data subject. This represents a new lack of control and a new set of risks.¹⁰¹

The way to mitigate these risks lies in a change in the paradigm that governs data retention. Those who retain data must rely not on the absence of a reason to delete but on a justification that legitimizes the continued retention. This means that, unless there is a legitimate reason for retaining the data, personal data must be deleted.¹⁰² Accordingly, for it to be possible to speak of individuals' autonomy over their personal data, the deletion of such data must be brought to the fore.

The notion that an individual must also possess autonomy over their personal data was first brought to the forefront by the German Federal Constitutional Court in its landmark decision of 15 December 1983, commonly known as the “Census” decision. The case concerned the Population Census Act, which allowed for the collection of significantly more data than a mere population count, raising concerns that such data could be misused beyond its intended purpose. These concerns were brought before the Constitutional Court. The Court, interpreting the concepts of human dignity and the right to personality enshrined in the German Basic Law, derived a new right from these two guarantees—namely, the “right to informational self-determination” (informelles Selbstbestimmungsrecht), thereby delivering a judgment far ahead of its time. The Court held that for an individual’s human dignity to be protected and for personal development to be possible, the individual must be able to exercise free control over their personal data. With this decision, it was affirmed that from the perspective of personal data protection, the individual's ability to control their own data is closely related to human dignity, individual freedom, and the right to dispose of one’s own personal data (information). It was also

¹⁰⁰ Bernal, 176.

¹⁰¹ Bernal, 176.

¹⁰² Bernal, 177. At this point, the author refers to the right to erasure and mentions its differences from the right to be forgotten. However, since the differences between the right to erasure and the right to be forgotten will be addressed later, the aim here is merely to explain the relationship between the concept of autonomy and the deletion of personal data.

emphasized that this is one of the prerequisites of a democratic society.¹⁰³ For the individual's autonomy over information not only serves to protect them from interventions in their personal data under data protection law but is also recognized as a precondition for citizens' impartial participation in the political processes of a democratic constitutional state.¹⁰⁴

Accordingly, following the protection of human dignity and the right to develop one's material and moral integrity—both of which are generally safeguarded by the right to be forgotten—it can be concluded that the right also protects, first and foremost, the data subject's right to dispose over their personal data. At this point, it seems unnecessary to separately address the general right to the protection of personal data, given that the subject matter of the right to be forgotten is, by definition, personal data itself. Therefore, it would be more appropriate to approach the matter from this perspective. Nonetheless, it should be stated that the right to be forgotten embodies all the aims of the right to the protection of personal data.

What distinguishes the right to be forgotten most significantly from the right to the protection of personal data is that it encompasses a psychological and philosophical dimension in terms of the data subject's need to forget. Of course, the basis of personal data protection also lies in the increasing transparency of individuals due to advancing technology and the negative impact of surveillance on individuals, and in this context, human dignity is also sought to be protected. However, what is protected within the scope of the right to be forgotten is this very psychological and philosophical approach in its own right. Consequently, another value protected by the right to be forgotten—specifically from the perspective of the data subject—is the ability to be forgotten.

As the individual's need to forget—and thereby to be forgotten—in order to live their life as they wish, without being bound by the burden of the past, has already been explained in detail above, we refrain from repetition here and limit ourselves to referring to the relevant section and emphasizing the significance of forgetting for the life of the individual.

3. Preventing Data Pollution

With the development of information technologies, the increase in the capacity of such tools, and the possibility of storing large amounts of data on very small devices, data—whether necessary or not—has begun to be retained.

¹⁰³ **Jef Ausloos**, *The Right to Erasure in EU Data Protection Law*, Oxford University Press, Oxford, 2020, 27, 28.

¹⁰⁴ **Gerrit Hornung/Christoph Schnabel**, "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self Determination", *Computer Law & Security Review*, Vol. 25, 2009, 86; **Ausloos**, 41.

Individuals now tend to store vast quantities of data, either with the thought of “perhaps I’ll come back to it later” despite no longer needing it, or anticipating a potential future need with the mindset of “let me keep it, I might need it later.” As a result, the phenomenon we today refer to as “data pollution” has emerged. One of the primary purposes of establishing the obligation to delete personal data and granting the data subject the direct right to request such deletion is precisely to eliminate this pollution and to prevent its further growth.

However, it should be noted that this objective also constitutes a fundamental basis of the right to the protection of personal data and is, in terms of the right to be forgotten, a subsequent and derivative purpose.

E. Scope

Although the right of the data subject to request erasure has also been provided for under Law No. 6698, the Law does not contain a detailed explanation as to the scope of this right. Therefore, the scope will be sought to be determined in light of the GDPR provisions and the above-mentioned decision of the Court. Accordingly, individuals shall have the right to request the erasure of their personal data and to prevent its processing under the following circumstances:

1. No longer necessary in relation to the purposes for which the personal data were collected or otherwise processed

It was previously explained that the data controller must comply with the principles of processing personal data for specified, explicit, and legitimate purposes, and retaining the data only for as long as necessary for those purposes. If the data subject becomes aware that this obligation has not been fulfilled, they have the right to request the erasure of the data, unless an exception applies.

In cases where the data controller processes personal data based on the data subject’s consent, if the data subject withdraws their consent and there is no other legal basis for the processing activity, the data controller is obliged to comply with this request and erase or destroy the personal data in question. The Court has defined such situations as instances where the data are no longer necessary for the purposes for which they were collected or processed, have become inadequate, irrelevant, or—considering the passage of time—“excessive” in relation to those purposes.

If the sole legal basis for the data controller's processing activity is the explicit consent of the data subject, the data subject may exercise the right to be forgotten upon withdrawal of that consent—provided there is no other legal ground for the processing. However, the data controller may process personal data based on other legal grounds as well. For instance, if some of the personal

data are necessary for the performance of a contract concluded with the data subject, the right to be forgotten cannot be applied to such data.¹⁰⁵

2. Objection by the Data Subject to the Processing Activity and Absence of an Overriding Legitimate Ground for the Processing Activity

The legal right of the data subject to object to the processing activity has been examined above. A data subject who exercises this right also has the right to request the erasure of the relevant data. However, it must be emphasized that although the right to object to the processing of personal data for direct marketing purposes is absolute, this does not necessarily trigger an absolute right to erasure. The right to be forgotten may not apply if the data controller has another legal basis for processing. For example, if the personal data processed for marketing purposes are also necessary for the performance of a contract with the data subject, the data subject cannot validly request the erasure of such data.¹⁰⁶

3. Illegal Processing of Personal Data

If the data subject becomes aware that their personal data has been or is currently being processed unlawfully, they may exercise the right to erasure in such circumstances. This right may apply if the data controller collects more data than necessary to achieve its purpose, fails to take the required measures by violating confidentiality obligations, or retains personal data longer than necessary for the specified purpose.

4. The Obligation to Delete Personal Data in Order to Comply with a Legal Obligation Applicable to the Data Controller

This situation will arise especially when the retention period of personal data is stipulated in the relevant legislation. For example, a data controller who is aware that personal data must be retained for five years according to the applicable law may exercise the right to erasure at the end of this period. Moreover, the data controller is already obliged to delete such data automatically after this retention period.

¹⁰⁵ At this point, it should be noted that although the data controller may have a legal basis for processing personal data, obtaining consent from the data subject despite this is considered unlawful under Law No. 6698. However, if a new legitimate purpose arises after the request for the right to be forgotten, this will not constitute a problem.

¹⁰⁶ Heledd Lloyd-Jones/Peter Carey, "The Rights of Individuals", Data Protection: A Practical Guide to UK Law, Ed. Peter Carey, 5. Ed., Oxford University Press, Oxford, 2018, 144.

5. The Personal Data Collected in Relation to the Provision of Online Services to Children

The GDPR places particular emphasis on the protection of personal data of children in connection with online services. This right protects children against the collection of consent for the processing of their personal data at a time when they may not be fully aware of all the risks that could subsequently arise from the processing of their data by online service providers and grants them the authority to request the deletion of such data thereafter.¹⁰⁷

The data controller, when obliged to delete personal data based on such requests or possibilities, must take reasonable steps, including the necessary technical measures, considering the current technology and implementation costs. However, data controllers should not forget that the right to erasure is not an absolute right and is subject to exceptions. For example, if a data controller is already legally obliged to process personal data and deletes the data in response to a deletion request, they may be held liable for failing to fulfil their legal obligation. Therefore, at this point, we believe it is more appropriate for data controllers to make the necessary assessment, taking into account the relevant legal regulations, regarding whether they are genuinely required to delete the concerned personal data, and only then proceed with the deletion.

F. Exceptions to the Right

One of the important issues concerning the right to be forgotten is the need to establish a balance between various rights. In this context, particular attention is given to the balance between the data subject's human dignity, the right to develop their material and moral integrity, and the right to the protection of personal data on the one hand, and the public's right to access information as well as the freedom of information providers to disseminate information on the other.

The fundamental conclusion drawn here, which we also share, is that the right to be forgotten is neither unlimited nor absolute. While we acknowledge this right, we believe that where it conflicts with other fundamental rights and freedoms, a balance must be struck, and absolute acceptance of the right to be forgotten should be avoided.

Since the relationship between the right to be forgotten and other fundamental rights and freedoms will be examined under a separate heading below, at this point we suffice with noting that the right is not absolute and that exceptions exist.

¹⁰⁷ Lloyd-Jones/Carey, 145.

G. Legal Basis Issue of the Right

It should be noted that there is currently no legal regulation that directly defines and protects the right to be forgotten, and only some preliminary studies have been initiated in this regard. As will be examined later, the only regulation that provides protection for the right is the GDPR provision, which addresses the right to be forgotten within the scope of the right to erasure. However, this provision is considered insufficient both because it does not directly define the right to be forgotten and because it fails to resolve the contentious issues surrounding the right.

Although the right to be forgotten has not yet been explicitly regulated, it is possible to recognize its normative existence through existing legal regulations due to its connection with related rights and freedoms. Undoubtedly, establishing a clear legal basis for the protection of a right is an important step in grounding it normatively. However, even if a newly emerging right has not yet been explicitly regulated in a normative source, it is possible to consider the emerging right within the scope of an existing right through broad interpretation of similar rights. In our view, in such a case, a right that is not legally regulated should also be considered under protection. This is precisely how protection for the right to be forgotten should be regarded at present.

As mentioned above, the right to be forgotten is regarded today as a necessary category of rights to realize human dignity—one of the fundamental aims of the field of human rights—and to ensure the development of an individual's material and moral existence. In this context, the existence of the right to be forgotten is an indispensable component for the adequate protection of the right to privacy and the protection of personal data, which are explicitly safeguarded by legal regulations.

Furthermore, the fact that the right has become the subject of concrete cases and that these cases have been accepted before judicial authorities, as explained above, has ensured that the issue is brought to the fore and protected through judicial precedents. Therefore, it would be incorrect to claim that the right to be forgotten has no normative basis. However, it is an undeniable fact that many points remain controversial and unclear.

Moreover, given the novelty of the right, even if indirect protection is accepted, this protection will soon prove insufficient in the face of rapidly evolving technology. For this reason, we believe that the right to be forgotten should be defined by legal regulations, its scope determined, and sufficient and necessary safeguards provided for this right. However, while doing so, the scope of the right should be clearly delineated, and the balance to be struck among

other fundamental rights and freedoms with which it may conflict should be determined with great care and precision.

III. The Relationship of the Right to Be Forgotten with Some Other Rights

The right to be forgotten interacts with many other rights due to its relation to personal data, its potential impact beyond the data subject to other individuals or society, and its close connection with information technologies. This characteristic of the right to be forgotten means that, while it may support or complement certain other rights, it also entails conflicts with various rights. This section focuses on the rights with which the right to be forgotten has either positive or negative interactions.

The right to be forgotten inevitably conflicts with other human rights or fundamental rights and freedoms such as freedom of expression, the right to information, property rights, or the right to engage in domestic or cross-border commercial activities. The limits of the right to be forgotten arise from the balance it must maintain with these rights; therefore, like many other categories of rights, the right to be forgotten is by no means unlimited in this sense. In this context, the recognition and acceptance of the right to be forgotten as a right depend on the legitimacy of its limitations in relation to other fundamental rights.¹⁰⁸

It should be noted that while there is no difficult area of agreement regarding rights that are similar to the right to be forgotten in terms of its purpose and the values it protects, there are many controversial and unclear points within the rights it conflicts with. Therefore, first, a brief mention will be made of the rights closely related to it, and then primarily the rights that conflict with the right to be forgotten will be addressed. This is because the intense criticism of the right and the criticisms regarding its non-application stem from these conflicts.

Neither the right to freedom of expression, nor the right to privacy, nor the right to be forgotten are inventions of the modern world. The intrinsic connection and balance between these rights have been tested for centuries and continue to be tested daily due to advancements in science and technology. Indeed, cases requesting the deletion of publicly available information were known to exist in the 1800s.¹⁰⁹ However, with the increase in digital storage capacity and the

¹⁰⁸ Werro, 2.

¹⁰⁹ Bkz. **Karen Eltis/Pierre Trudel**, Canadian Report: Delisting in the Digital Age – A Hybrid Approach to Bridge the European and American Visions of the “Right to be Forgotten”, International Academy of Comparative Law - Fukuoka Congress, 2018, 3. See also. **Amy Gajda**, “Privacy, Press, and the Right to Be Forgotten in the United States”, Washington Law Review, Vol. 93, 2018, 201-264.

emergence of the internet allowing instant and widespread communication, the frequency of conversations, images, and appearances that an individual wishes to keep private has increased. Traditionally, the four walls of an individual's home have been considered the boundary for investigations by third parties and the state. However, frankly, in the digital world, the adequacy of this physical boundary is questioned, as the proliferation of the internet has threatened the privacy of private life more than ever before. The individual's home no longer provides the necessary boundaries for full protection against invasions of privacy.¹¹⁰

The right to be forgotten will be examined by considering rights that both share the same purpose and function as well as those that are in direct opposition, seeking to answer whether this right should be accepted absolutely, not accepted at all, or positioned in a balance among these rights, thereby attempting to understand where the right should stand.

A. Rights Related to the Right to Be Forgotten

It should be noted that the rights supporting the right to be forgotten have already been examined in detail throughout the entire study, particularly under the headings of the elements of the right and the values it protects. Therefore, at this point, we will limit ourselves to a brief reminder and refer to the relevant sections to avoid repetition.

1. In Terms of the Concept of Human Rights

Here, rather than discussing whether the right to be forgotten should be regarded as a human right, it is necessary to emphasize, as mentioned above, the close relationship of the right to be forgotten with the fundamental concepts of the human rights domain.

Human rights, above all, are based on the right of the individual to develop their material and spiritual integrity. They link the rights that an individual possesses simply by being human to the rights that they must have in order to be able to develop their material and spiritual integrity. On the other hand, the realization of human rights also requires the principle of human dignity. An individual must be able to exist in a manner worthy of human dignity in order to protect and develop their personality.

Here, the relationship of the right to be forgotten with the field of human rights is clearly seen. With the right to be forgotten, the individual sets aside past negativities, carries the hope of a new beginning, and thus demands the

¹¹⁰ Werro, s. 19.

protection of their material and spiritual integrity over their past, present, and future.¹¹¹

The European Court of Human Rights (ECtHR) explains the essence of the Convention as respect for human dignity and human freedom. Within this scope, personal autonomy is a fundamental principle underlying these protections. Every individual's personal sphere, including all rights related to their identity, must be afforded the necessary protection.¹¹² Therefore, the Court characterizes the concept of personal autonomy as an essential element within the guarantees provided by the Convention and concludes that protecting the individual's personal sphere is necessary to ensure this. For this purpose, it is clear that personal data, which constitutes the largest part of an individual's personal sphere, must be adequately protected, and the individual must be granted autonomy over this area. The right to be forgotten also rests on an individual's autonomy to hold rights over their personal data over time.¹¹³

The protection of human dignity and reputation is also one of the concepts aimed at by the right to be forgotten. Indeed, the occurrence of an event that a person wishes to be forgotten does not mean that the person's dignity and reputation cannot be protected.¹¹⁴

2. The Protection of Private Life

After the general topic of human rights, the protection of private life stands as the most comprehensive and extensive fundamental right and freedom that shares similar purposes and values with the right to be forgotten. As previously noted, there are views suggesting that the right to be forgotten should be considered a component of the right to private life protection. Moreover, although the right to the protection of personal data is now recognized as an independent right, it is still often treated under the umbrella of private life protection. A fundamental example of this is the ECtHR evaluating relevant cases under Article 8 of the Convention, which concerns the protection of private life.

Therefore, despite differing opinions regarding the scope, nature, and independence of these rights, their close relationship in terms of purpose and values is undeniable and incontestable. For this reason, among the rights interacting with the right to be forgotten, the protection of private life and even

¹¹¹ **Turgut**, 121. See also. **Olgun Değirmenci**, Yargısal İçtihatların Ortaya Çıkardığı Bir Hak: Unutulma Hakkı (Çerçevesi ve Hak Üzerine Düşünceler), *Terazi Hukuk Dergisi*, C. 13, S. 144, Ağustos, 2018, 155.

¹¹² *Christine Goodwin v. Birleşik Krallık*, 28957/95, 11.07.2002, § 90. See also, in a similar vein. *Pretty v. Birleşik Krallık*, 2346/02, 29.04.2002, § 62.

¹¹³ **Weber**, 121.

¹¹⁴ **Turgut**, 124.

its subcategories must be addressed. However, there is no need here to provide a detailed explanation of the concept of private life or this right. Instead, a general framework of private life protection will be outlined, and the place and significance of the right to be forgotten within this framework will be determined. Thus, explanations will focus solely on clarifying the relationship between the right to be forgotten and the right to private life.

a. General Protection of Private Life and the Right to be Forgotten

The concept of private life refers to a complex and extensive area that cannot be precisely defined or limited.¹¹⁵ Indeed, the ECtHR rulings have avoided defining private life explicitly in order to prevent the limitation of the concept.

The Court, in its judgment in “*Niemietz v. Germany*”¹¹⁶ holds the view that providing a comprehensive definition of the concept of private life is neither possible nor necessary.¹¹⁷ However, it notes that restricting the concept to an “inner area” where the individual can live their private life as they wish, and completely excluding the outside world beyond this area, would be excessively restrictive. The Court states that the right to private life should, to a certain extent, also include establishing and maintaining relationships with other people. Accordingly, the Court explicitly affirms that private life must include, for example, the “*right to establish and develop relationships with others*”.¹¹⁸

The Court, in the case of “*Costello – Roberts v. United Kingdom*”,¹¹⁹ similarly concluded that the concept of private life is too broad to be explained in detail and with precision. It characterized this concept as broader than privacy, encompassing a realm where every individual can freely form and develop their personality and which also includes the individual's relationship with the outside world.¹²⁰

¹¹⁵ For an analysis of the impact of the right to respect for private life on the right to be forgotten within the framework of the sphere theory (public sphere, private sphere, and intimate/confidential sphere), see. **Turgut**, 129 – 141.

¹¹⁶ *Niemietz v. Almanya*, 13710/88, 16.12.1992, § 29.

¹¹⁷ **Gilles Dutertre**, *Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler*, Avrupa Konseyi Yayınları, Strazburg, 2013, 201.

¹¹⁸ **Orla Lynskey**, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015, 106.

¹¹⁹ *Costello – Roberts v. Birleşik Krallık*, 13134/87, 26.03.1993.

¹²⁰ **Ivana Roagna**, *Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması*, Avrupa Konseyi İnsan Hakları El Kitapları, Avrupa Konseyi Yayını, Strazburg, 2012, 12.

b. Privacy

An individual's privacy is the cornerstone of the protection of private life. Above all, the individual's private sphere must be safeguarded. Privacy constitutes an indispensable domain for individuals. Indeed, a survey conducted in the United States concerning social networking sites concluded that participants exhibited significant concern and perceived danger regarding their private data, while simultaneously experiencing a lack of control over it.¹²¹

Therefore, it is evident that the individual's expectations regarding privacy relate to the personal data that is the subject matter of the right to be forgotten. Although this can be definitively stated for the right to privacy of private life, there are debates within the scope of the right to privacy. The right to privacy protects data that individuals do not wish to disclose publicly. However, the right to be forgotten deals with information that has already been made public. Consequently, it is technically argued that the right to be forgotten cannot be protected under the right to privacy.¹²²

c. Protection of Reputation

The protection of an individual's reputation is a fundamental right addressed either directly or within the scope of the protection of private life by key national and international regulations. The ECtHR considers the protection of reputation within the context of Article 8 of the Convention, which safeguards private life.

The Court's judgment in "*Karakó v. Hungary*",¹²³ which contains important statements and opinions regarding the protection of reputation, is significant in this respect. According to the Court, personal rights and the integrity of personality covered under Article 8 of the Convention are not related to the external assessment of the individual. However, in terms of reputation, this external assessment is decisive: A person may lose the respect of society, regardless of whether it is justified, but the integrity of the individual cannot be lost or transferred. According to the Court's case law, reputation can sometimes be recognized as an independent right; it is mostly protected when the allegations are entirely true, constitute an attack, and have an inevitable direct impact on the applicant's private life.

¹²¹ **Roger Taylor**, "No Privacy without Transparency", *Data Protection and Privacy: The Age of Intelligent Machines*, Ed. Ronald Leenes/Rosamunde van Brakel/Serge Gutwirth/Paul De Hert, Hart Publishing, Oxford, 2017, 66. See also. **Susan B. Barnes**, *A Privacy Paradox: Social Networking in the United States*, 2006, <https://firstmonday.org/ojs/index.php/fm/article/view/1394>. 23.05.2020.

¹²² **Sözüer**, 60.

¹²³ *Karakó v. Macaristan*, 39311/05, 28.04.2009, § 23.

In our view, the most important aspect of the judgment is not only its definition of the nature of reputation but also its comparison with freedom of expression. According to the Court, Article 10 of the Convention, which regulates freedom of expression, may be restricted to protect reputation. Moreover, the Court holds that the article itself allows for such restrictions. Therefore, according to the Court, the phrase “the rights of others” in the second paragraph of Article 10 encompasses personal integrity rights, and restrictions made to protect private life, provided they are proportionate, can form the basis for limiting freedom of expression.¹²⁴

The content subject to the right to be forgotten concerning the reputation of the data subject is significant in evaluating whether the right should be applied. Typically, a person desires the erasure of information that damages their reputation and cites this reason when exercising the right to be forgotten. Most importantly, this reasoning is justified. It is a behaviour that can be expected from a person in the normal course of life to wish for the erasure of information that harms their reputation. Therefore, the concept of protecting a person's reputation, considered within the scope of the right to privacy, is closely related to the right to be forgotten.

3. Right to the Protection of Personal Data

The right to the protection of personal data is the area most closely related to the right to be forgotten in every respect. The need for both rights arise from similar reasons, their connection with information technologies, and the significance of the digital environment. The shared purpose and protected values make it impossible to separate the two rights from each other. Indeed, the right to be forgotten is considered a complementary element, component, or subsection of the right to the protection of personal data.

Moreover, the most important point here is that the subject of the right to be forgotten is personal data, since the personal data for which access is sought to be blocked through the exercise of this right. Therefore, the right to the protection of personal data undoubtedly finds a place in all stages of the right to be forgotten.

However, since this relationship has been addressed throughout the study and references to the right to the protection of personal data have been made as necessary, here we only make reference to the relevant sections and emphasize the importance, scope, and degree of this relationship.

¹²⁴ Karakó v. Macaristan, § 24, 25.

B. The Rights and Concepts in Conflict with the Right to be Forgotten

1. Concept of Historicity

When viewed from a broader perspective than fundamental rights and freedoms, one of the greatest dilemmas of the right to be forgotten is the phenomenon of “historicity.” If a person who does not want to bear the burden of their past is accepted to be part of history, the individual’s request conflicts with the preservation of history.

Indeed, the request of the murderers of the German actor Walter Sedlmayr to remove their criminal records from Sedlmayr’s Wikipedia page is genuinely an attempt to “*rewrite history*”.¹²⁵ However, this request was initially rejected by the German Federal Court, and the subsequent application for violation of rights was deemed inadmissible by the ECtHR. As a result of these decisions, the names of the convicted brothers were reinstated on the German-language Wikipedia page. Therefore, personal data that forms historical and social consciousness was prevented from benefiting from the right to be forgotten.

2. Freedom of Expression

The core point of the criticisms regarding the right to be forgotten is gathered under the heading of the right to freedom of expression. Freedom of expression is a fundamental right protected by all national and international regulations concerning fundamental rights and freedoms, and there are concerns that the right to be forgotten may harm this right due to its conflict with it. Therefore, there are views advocating that the right to be forgotten should not be accepted, or if it is to be accepted, it should be addressed in a manner that does not conflict with freedom of expression. To clarify these criticisms, the concept of freedom of expression should be understood and the matters covered by its scope clearly determined. Thus, the points at which the right to be forgotten conflicts with freedom of expression can be identified.

Fundamentally, freedom of expression, protected under Article 10 of the The European Convention on Human Rights (ECHR), has been comprehensively examined in the ECtHR’s decision in “*Stoll v. Switzerland*”.¹²⁶ According to this decision, freedom of expression is one of the fundamental pillars of a democratic society and is accepted as a basic condition for the development of both the individual and society. According to the second paragraph of the relevant article, this freedom applies not only to “positive” speech or trivial and uninteresting matters but also to ideas and information that

¹²⁵ Bernal, 201.

¹²⁶ Stoll v. İsviçre, 69698/01, 10.12.2007, § 101.

may be inappropriate, shocking, or disturbing. These constitute the conditions of pluralism, tolerance, and broad-mindedness, without which there can be no democratic society. Although this freedom, like other fundamental rights and freedoms, is subject to exceptions, it must be interpreted broadly, and any grounds for restriction must be convincingly justified.¹²⁷ Moreover, it should not be forgotten that limitations on freedom of expression have boundaries, which must meet the requirements of necessity and proportionality in a democratic society.

Freedom of expression refers to the free disclosure of information or ideas and the unrestricted access to such information or ideas. Within this scope, the freedom of the content of the expression, the subject of the expression, and the means through which the expression is provided or accessed must be ensured as a whole. The absence of any one of these elements prevents the effective protection of freedom of expression.

Freedom of expression includes the free disclosure of information or ideas. Disclosure of information encompasses the freedoms of dissemination and provision of information as well. Therefore, individuals, institutions, or organizations engaged in providing information activities must be regarded and protected within the scope of freedom of expression. In this context, the importance of press and broadcasting organizations is evident.

Indeed, the ECtHR has considered freedom of the press within the scope of freedom of expression due to its role in providing information. Accordingly, press and broadcasting organizations and their sources must be protected by laws in a manner that realizes press freedom. Without such protection, public information on matters beneficial to society would be hindered. Therefore, the protection of the press is of utmost importance for public awareness and for the press's ability to provide accurate and reliable information. Interference with press freedom in a democratic society is a chilling and incompatible practice with freedom of expression.¹²⁸

The advancement of technology has transformed the internet into the most significant tool for the dissemination of information. This development has been elevated to a higher level with Web 2.0 technology, which allows individuals to share content themselves. Therefore, the right to be forgotten is also connected

¹²⁷ See also, in a similar vein. *Animal Defenders International v. Birleşik Krallık*, 48876/08, 22.04.2013 § 100; *Morice v. Fransa*, 29369/10, 23.04.2015, § 124.

¹²⁸ *Goodwin v. Birleşik Krallık*, 5493/72, 27.03.1996, § 39.

to Web 2.0. Web 2.0 enables interactive activities, allowing people to share information, pictures, and videos, or more generally, to express themselves.¹²⁹

Therefore, nowadays, not only press organizations but also individuals occupy the information-providing side of freedom of expression through disseminating and sharing information. The ECtHR states that freedom of expression is a right granted to everyone and, consequently, it should not only protect organizations such as the press and media but also real persons.¹³⁰ For this reason, everyone providing information and content, whether natural or legal persons, must be protected within the scope of freedom of expression.

The ECtHR has described the internet, especially following user-generated content, as a “unique platform from the perspective of freedom of expression”.¹³¹ Consequently, today the internet is regarded as one of the largest instruments where freedom of expression comes into play. Therefore, both the press and the internet must be protected within the scope of freedom of expression. The effective protection of freedom of expression encompasses not only the expression itself but also the medium through which this expression is articulated, explained, or disseminated.

In conclusion, there is no doubt that the internet is one of the most fundamental sources for ensuring and protecting freedom of expression. Regarding the right to be forgotten, it is necessary to take a step further and examine the role of search engines within freedom of expression: Are search engines also considered information providers from the standpoint of freedom of expression? It should be noted that although search engines do not directly disseminate information, they act as intermediaries in the spreading of information. As stated above, since the means through which expression is conveyed are also encompassed by freedom of expression, search engines must be included under freedom of expression as tools used to disseminate information.

Opposite the inclusion of information provision under freedom of expression is the right to access information. For individuals to acquire information, they must have access to it. The essential understanding here is not that an individual subjectively desires to access any information based on personal reasons, but rather the freedom of society to acquire and access information. Here, the connection of this right with “public interest” emerges. The ability of everyone to freely access and acquire information about matters

¹²⁹ **de Terwangne**, 90.

¹³⁰ *Autronic AG v. İsviçre*, 12726/87, 22.05.1990, § 47. See also. *Sunday Times v. Birleşik Krallık*, 6538/74, 26.04.1979.

¹³¹ *Delfi AS v. Estonya*, 64569/09, 16.06.2015, § 101.

objectively concerning the entire society depends on whether there is a “public interest”. It is clear that when public interest is acknowledged, the right to access information receives broader protection.

In the relationship to be established with the right to be forgotten, the information that the data subject requests to block access to and wishes to be forgotten comes into conflict with another individual's right to access. Here, the concept of public interest mentioned above is crucial. It is inconceivable to protect a situation in which one individual does not want access to their personal data while another person wants to access this information for their own personal reasons. What must be discussed and what truly confronts each other is what the personal data in question means in terms of the concept of public interest regarding the right to be forgotten: In this context, the question is whether the right to the protection of personal data or the public interest will prevail. Due to the confrontation of these two important interests, we believe that, first and foremost, the content and scope of these concepts should be clearly and explicitly identified.

The conflicting situation between the right to be forgotten and freedom of expression begins precisely at this point. What is intended to be achieved with the right to be forgotten is the removal of personal information upon the request of the data subject and the prevention of others from accessing this information. Therefore, the fulfilment of a data subject's right to be forgotten necessarily involves an intervention in freedom of expression through the obstruction of information provision and access.

Therefore, it is considered that freedom of expression should have a limit in this regard. Accordingly, there are a few situations where data protection norms do not require the protection of any confidentiality. Freedom of expression should be approached similarly within the scope of the right to information and access to information. In such a case, the processing of personal data is unlikely to go hand in hand with the strengthening of individuals' rights and interests. According to the EU directive on the reuse of public sector information, freedom of communication and the right to information, freedom of expression and freedom of access to official documents, participatory democracy, and the functioning of the internal market depend on the free movement of services and information.¹³²

The rights concerning the confidentiality and security of data are distinguished from other rights, especially freedom of expression under the

¹³² **Ugo Pagallo**, “The Impact of Domestic Robots on Privacy and Data Protection, and the Troubles with Legal Regulation by Design”, *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Ed. Serge Gutwirth/Ronald Leenes/Paul De Hert, Springer, Heidelberg, 2016, 399.

Convention, by generally providing protection aimed at individual interests. Freedom of expression, while connected to personal expression and development, is also linked to societal interests such as the presence of ideas in public spheres, the proper functioning of the press, truthful investigations, and being a prerequisite for democracy. According to the prevailing view, Article 8 of the Convention, which regulates the protection of private life, primarily protects individual interests such as autonomy, dignity, and personal development.¹³³

Thus, it must be accepted that the right to privacy has a material scope. Article 8 of the Convention, in principle, provides protection for a person's private life, family life, correspondence, and home life.¹³⁴ However, it is also useful to note in the doctrine that the public dimension of privacy is increasingly being recognized.¹³⁵ The ECtHR states that the right to privacy also protects an individual's personal development, includes protection from environmental interventions, and may extend to data protection matters.¹³⁶

This distinction related to individual interests also significantly impacts the types of applicants who may lodge complaints concerning the right to privacy. The Convention, in principle, allows natural persons, groups of persons, and legal persons to complain about violations of their rights under the Convention. Indeed, the ECtHR has accepted that churches may claim freedom of religion (Article 9 ECHR), press organizations are protected under freedom of expression (Article 10 ECHR), and trade unions may have their freedom of assembly and association protected under freedom of expression (Article 11 ECHR) when they assert these claims.¹³⁷

However, the Court states that Article 8 ECHR primarily protects individual interests and, as a rule, only natural persons can invoke rights to privacy and confidentiality. For example, when a church requests police protection out of concern for the violation of its confidentiality in a criminal case, the extent to which a non-governmental organization may enjoy such a right must be determined considering the unique nature of the right itself.¹³⁸

¹³³ **Bart van der Sloot**, "Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities", *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Ed. Serge Gutwirth/Ronald Leenes/Paul De Hert, Springer, Heidelberg, 2016, 417, 418.

¹³⁴ **Pagallo**, 399.

¹³⁵ **van der Sloot**, 418.

¹³⁶ *Leander v. İsveç*, 9248/81, 26.03.1987; *Amann v. İsveç*, 27798/95, 16.02.2000; *Rotaru v. Romanya*, 28341/95, 04.05.2000.

¹³⁷ **van der Sloot**, 418.

¹³⁸ **van der Sloot**, 418.

It is true that a church has, under Article 9 of the Convention, the right of its members and representatives to freedom of religion, to exercise this freedom, and to demand it in all the church's operations, and that everyone must respect this right. However, Article 8 of the Convention, by contrast, concerns an individual rather than a collective character or understanding.¹³⁹ Therefore, the Court has treated this as a matter of case law and deemed complaints outside this line inadmissible. It has stated that deviation from this line is only possible in exceptional circumstances: *“Essentially, claims by groups of natural persons alleging a violation of a right recognized in the Convention have been rejected by the Court, and interstate complaints are rarely pursued (Article 33 ECHR). This leaves open only the possibility of an individual complaint for violation of privacy rights.”*¹⁴⁰

At this point, the problem is that focusing on natural persons and individual harm makes protection difficult in situations that do not concern a specific individual but affect large groups in society and potentially everyone. Given the increasing trend toward the use of large data collection systems, interest in big data cases is likely to increase. In such cases, the ECtHR faces the options of adhering to a strict interpretation of the victim's individual interests and declaring the case inadmissible; acknowledging that such cases fall within its jurisdiction and moving away from or expanding the focus on individual harm.¹⁴¹

The Court generally opts for the second option in the following three situations:

- When the applicant has a reasonable likelihood of suffering harm,
- When the applicant has a high likelihood of being affected by the practice in the future,
- When the mere existence of such a law or policy results in a violation of Article 8 of the ECHR.¹⁴²

Here, concerns arise that the differences between the right to be forgotten and freedom of expression may lead to censorship. Indeed, some explain this by stating that there needs to be greater clarity on how the right to be forgotten can be implemented, while others, referring to the Court's decision discussed above, believe that the EU has effectively asked Google to censor the web. At this point,

¹³⁹ Stes Colas Estand others v. Fransa, 37971/97, 16.04.2002.

¹⁴⁰ **ven der Sloot**, 418, 419.

¹⁴¹ X. v. İzlanda, 6825/74, 18.05.1976.

¹⁴² **ven der Sloot**, 419.

concerns converge on the idea that the internet may no longer be as free and open as it currently is.¹⁴³

Peter Fleischer, Google's privacy counsel, has highlighted that the right to be forgotten and the right to request information deletion are very current trends, noting that data protection is increasingly being used as a justification for online censorship practices, which raises the danger of creating a ground for censorship.¹⁴⁴

In light of all these explanations, the primary understanding that must be reached is that there is uncertainty about how, specifically on the internet and more generally for freedom of expression, rights such as the right to be forgotten can coexist, be used, and be implemented. Therefore, in our opinion, the first step should be to develop ideas and arguments to address this deficiency. Thus, by establishing a balance between the right to be forgotten and other rights and concepts that contain conflicting points, it should be clearly determined how all these concepts can coexist, be used, and be implemented together.

When processing personal data based on grounds other than the data subject's consent, the interests of the data subject, protected by the right to be forgotten, may conflict with other interests, rights, and freedoms: The interests of the data processor or those involved in such processing, or certain public interests, especially freedom of expression and freedom of the press, may conflict with it. Therefore, the unlimited application of the right to be forgotten prevents the full preservation and integrity of archives. For the same reason, it may conflict with the duty to preserve collective memory. It can obstruct historical research. Additionally, it affects business continuity, management of employee files, the duty to preserve evidence, and inevitably, in the context of exercising this right, the obligation to retain data for public security purposes must also be taken into account.¹⁴⁵

C. Balancing the Right to Be Forgotten with Other Rights and Concepts

Above, we attempted to explain the relationship of the right to be forgotten with rights and concepts that both share similar aims and values, as well as those that conflict with it. Rights and freedoms aligned with the same objectives do not pose obstacles to the implementation of the right to be forgotten; however,

¹⁴³ **Pereira/Vesnić-Alujevića/Ghezzi**, 14.

¹⁴⁴ **Peter Fleischer**, "The Right to be Forgotten, or How to Edit Your History" <http://peterfleischer.blogspot.com/2012/01/right-to-be-forgotten-or-how-to-edit.html>, 23.05.2020.

¹⁴⁵ **Cécile de Terwangne/Jean-Philippe Moïny**, Report on the Consultation on the Modernisation of Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg, 2011. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/TPDBUR_2011_10_en.pdf. 23.05.2020.

this is not the case for conflicting rights. These rights are endangered and compromised in various ways when the right to be forgotten is exercised.

So, what should be done in such cases? Should the right to be forgotten being disregarded and not recognized? Should efforts be made to balance the right to be forgotten with conflicting rights and interests so they can coexist? Or should the right to be forgotten being fully accepted even if it means overlooking the infringement of other rights?

The most reasonable choice appears to be the second option. Today, the need for the right to be forgotten has been thoroughly detailed above, considering both the importance of forgetting in human life and the impact of personal data in the digital environment. Although its scope and limits are not yet clearly defined, the existence of such a right should, in our view, be acknowledged. Indeed, decisions by the Court of Justice and other judicial bodies demonstrate this recognition. However, as emphasized above, the importance of freedom of expression—especially its societal dimension—and the concept of historicity must not be compromised.

In conclusion, neither the right to be forgotten nor the freedom of expression can be relinquished. Therefore, what must be done is to comprehensively address the right to be forgotten alongside other rights and freedoms and ensure their coexistence. Under this heading, we will provide explanations regarding the balance to be struck between the right to be forgotten and conflicting interests and endeavour to clarify the issue.

However, it must first be noted that establishing this balance is undoubtedly easier said than done. There are several reasons for this. Primarily, the possibility of implementing multiple rights and interests without harm to any of them requires clear and precise rules on how such implementation should occur. Ambiguity in this regard implies that the rights are at risk. Moreover, it is impossible to definitively determine in advance which concept—whether the right to be forgotten or freedom of expression—will prevail, or under which circumstances the right to be forgotten can be applied. This certainty can only be established based on the nature of the specific case.

Key factors to consider include the current legality of the personal data subject to the right to be forgotten, the nature of the data, the environment in which it exists, the passage of time, and, importantly, the relationship of this information to the concepts of the right to access information and freedom to provide information under freedom of expression, as well as its relevance to the public. Therefore, a prediction such as *“in this case freedom of expression shall prevail; in that case, the right to be forgotten applies and access to the information is blocked”* is neither feasible nor a correct approach. Accordingly,

rather than establishing definitive and strict lines, this section aims to identify the considerations and criteria that should be taken into account when balancing the right to be forgotten with other rights and freedoms.

1. The Balance Between the Right to be Forgotten and Freedom of Expression

To better understand which matters can be taken into account in establishing the balance, the following questions must first be clarified:

a. Is the Right to Be Forgotten an Absolute Right?

To determine how the right to be forgotten should be balanced, it is first necessary to examine its nature in terms of whether it is an absolute right. As previously mentioned, this right is not absolute and is subject to exceptions. Indeed, considering the importance and nature of the rights and freedoms with which the right to be forgotten especially conflicts, it cannot be protected in an entirely unrestricted manner.

According to Article 17 of the GDPR, which regulates the right to erasure, and the exceptions to this right listed in paragraph 3 of the same article, the information subject to the right to be forgotten cannot be deleted unless it is deemed necessary for the exercise of freedom of expression and information rights as stated in Article 17(3)(a). A similar provision was also found in Article 9 and Recitals 17 and 37 of Directive 95/46/EC. However, the GDPR includes the term “academic purposes”, which was not present in Directive 95/46/EC. Accordingly, the right to erasure is not applied to the extent necessary in the following cases:

- The exercise of the right to freedom of expression and information.
- Compliance with a legal obligation under Union or Member State law to which the data controller is subject, or the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For reasons of public interest in the area of public health as referred to in Articles 9(2)(h) and (i) and Article 9(3).
- Where the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1), insofar as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.
- For the establishment, exercise, or defense of legal claims.

On the other hand, it has been clearly stated that the right to be forgotten is not an absolute right. In this context, it has been explained that it must be

restricted particularly when it conflicts with the rights to freedom of expression and information. Moreover, if the personal data subject to the erasure request must be processed legally, for the public interest, scientific or historical research purposes, statistical purposes, archiving, or for the establishment, exercise, or defense of legal claims, the right to be forgotten will not apply in these cases.

The situation is similar in Turkish law. Article 28, titled “Exceptions”, which regulates the exact exceptions in Law No. 6698, specifies the cases in which the provisions of the Law will not apply. The article excludes from the scope of the Law personal data processed particularly in conflict with the right to be forgotten, such as those processed for freedom of expression, scientific and historical research, public order and interest purposes, and by judicial authorities. Therefore, these cases should also be considered the limits of the right to be forgotten under the Law.

Furthermore, in the Guide on the Right to Be Forgotten (Evaluation of the Right to Be Forgotten Regarding Search Engines) published by the Turkish Personal Data Protection Board, it is also stated that the right to be forgotten is not an absolute right that can be asserted by relevant persons under all conditions; rather, it is an exceptional right and therefore decisions must be made based on evaluations within criteria for each concrete case.¹⁴⁶

Thus, it is clear that the right to be forgotten is also subject to limitations according to the conditions to which the processing of personal data is subject. Although the cases where the right to be forgotten will not apply can be determined through legal provisions, we consider this insufficient.

First of all, we believe that these limitations should be kept quite broad. Nowadays, it is acknowledged and accepted that no activity, from daily life to professional operations, can be properly conducted without the processing of personal data; however, we also consider that this must be subject to defined rules without harming the essence of the right. Setting a rule and then rendering it almost ineffective by the exceptions applied to it is meaningless. In this context, if such an attitude is adopted, it will only appear that personal data is being protected and the right to be forgotten is being ensured, without actually achieving it. Therefore, great care must be taken regarding the imposed limitations. Excessive exceptions limiting the use of the right and expressing these exceptions with very general and repetitive concepts cannot provide adequate protection.

¹⁴⁶ KVKK, Unutulma Hakkı (Unutulma Hakkının Arama Motorları Üzerinde Değerlendirilmesi) Rehberi, 22. (The Guide on the Right to Be Forgotten (Evaluation of the Right to Be Forgotten in the Context of Search Engines), published by the Personal Data Protection Authority [KVKK]).

On the other hand, the legal basis of the right to be forgotten is weak and not directly protected, which likewise shows that the exceptions to the right are not clearly defined. It should be emphasized that the exceptions mentioned above are essentially those applied to the right of erasure. Thus, the current limitations imposed considering the essence of the right to be forgotten do not exist. For example, exception cases directly addressing the impact of personal data on the internet environment, public interest, and the data subject's position are not currently available.

For instance, in the “*M.L. and W.W. v. Germany*” case, the ECtHR rejected the applicants’ request, ruling that the public's overriding interest and benefit in obtaining information outweighed the right to be forgotten in the concrete case. It also found no violation of rights in the judgment delivered by the German Federal Court. Therefore, this decision clearly shows that the right to be forgotten is not an absolute right.

It is seen that GDPR contains necessary regulations to prevent the right to be forgotten from being prioritized over freedom of expression and the press's right to provide information. Accordingly, except for the exception in Article 17(3), Article 85 of GDPR emphasizes that member states should regulate the processing of personal data for journalistic purposes and for academic, artistic, and literary purposes. According to Article 2(2)(c) of GDPR, when personal data is processed entirely by a natural person in the course of purely personal or household activities, GDPR’s protection mechanisms do not apply. Therefore, these provisions should be considered as mechanisms preventing the right to be forgotten from taking precedence over the right to freedom of expression.

In conclusion, there is no doubt that the right to be forgotten is not absolute and, moreover, cannot be absolute given the rights and concepts it conflicts with. Although it may not be possible to limit with precise lines in which cases it will not be absolute and it requires looking at the specifics of the concrete case, we consider that specific and appropriate limitation cases should be introduced by taking into account the objectives and values protected by the right.

b. Is Freedom of Expression Subject to Restrictions?

The right to be forgotten is not absolute; thus, the limits of freedom of expression must also be examined. Freedom of expression, like many other fundamental rights and freedoms, is not absolute and can be restricted under certain circumstances. Therefore, it can be said that neither the right to be forgotten nor freedom of expression is absolute. However, while the right to be forgotten is subject to broad and numerous exceptions, freedom of expression is subject to the provisions regulating the limitation of fundamental rights and

freedoms. Consequently, any limitation imposed on freedom of expression is considerably narrower in scope.

For a restriction on freedom of expression to be valid, the interference must be prescribed by law, the reasons for the restriction must be interpreted narrowly, and it must be necessary and proportionate in a democratic society. This issue was thoroughly discussed in the ECtHR decision in “*S. and Marper v. United Kingdom*.”¹⁴⁷ According to this ruling, any interference must first be deemed “necessary in a democratic society.” The interference must pursue a legitimate aim and respond to a social need. Furthermore, the means employed to achieve the aim must be proportionate to the restriction imposed on the right. National authorities’ actions must be adequate and necessary within this context.

In its judgment in “*Christine Goodwin v. the United Kingdom*”,¹⁴⁸ the ECtHR stated that, in light of the diversity in the practices of the member states, the nature of interferences and the interpretation of legal concepts may vary from case to case, thereby affording national authorities a wide margin of appreciation.¹⁴⁹ However, the Court emphasized that, in any interference with fundamental rights and freedoms, a fair balance must be struck between the general interests of society and the interests of the individual. In line with its established case law, the Court highlighted the principles of legitimate justification, foreseeability under the law, and equality. It underlined that, under all circumstances and above all, the protection of human rights must constitute the primary consideration.¹⁵⁰

The scope of this wide margin of appreciation afforded to member states was elaborated in the *S. and Marper* judgment. According to the Court, the breadth of discretion depends on several factors, such as the nature of the right in question, its importance to the individual, and the nature, method, and purpose of the interference. This margin of appreciation is to be more narrowly construed particularly in cases where the right in question is of critical importance to the individual’s privacy.¹⁵¹

As a result, while freedom of expression constitutes a fundamental element for the establishment and development of a democratic society, it is not absolute and may be restricted under certain circumstances. However, for such

¹⁴⁷ *S. and Marper v. United Kingdom*, 30562/04, 30566/04, 04.12.2008, § 101.

¹⁴⁸ *Christine Goodwin v. United Kingdom*, 28957/95, 11.07.2002, § 72.

¹⁴⁹ *Cossey v. United Kingdom*, 27.09.1990, Serie A No. 184, 15, § 37

¹⁵⁰ *Christine Goodwin v. United Kingdom*, § 73. See also, in a similar vein. *Chapman v. United Kingdom* [GC], No. 27238/95, ECHR 2001-I, § 70.

¹⁵¹ *S. and Marper v. United Kingdom*, § 102. See also, in a similar vein. *Connors v. United Kingdom*, 66746/01, 27.05.2004, § 82.

restrictions to be deemed lawful, they must meet a number of distinct requirements mentioned above. Therefore, although freedom of expression, like the right to be forgotten, is subject to certain limitations, it must be noted that such restrictions are considerably narrower in scope compared to those applicable to the right to be forgotten.

2. Considerations in the Balancing of Rights

In light of the foregoing explanations, while the exercise and application of the right to be forgotten poses no issues in relation to rights that protect similar purposes and values, there are certain obstacles when it comes to rights and concepts that are in conflict with it. These obstacles have been addressed above. However, due to the need for the right to be forgotten, it is not possible to completely renounce this right merely on the basis of such conflicts. Therefore, a balance must be established between conflicting rights and concepts without undermining the essence of any right, and in doing so, the highest and most fundamental interest to be protected in the specific case must be identified and pursued accordingly.

This is, of course, a matter that cannot be precisely and definitively delineated in advance. Nevertheless, identifying the criteria to be considered in establishing this balance constitutes the first and fundamental step. Under this heading, based on the view that the right to be forgotten has become a necessity in today's world, an effort will be made to clarify the considerations that may serve to establish a balance in cases where this right conflicts with other rights and concepts, in order to ensure its appropriate implementation and exercise.

a. Determining the Scope of the Right to Be Forgotten

Determining the scope of the right to be forgotten is of vital importance in terms of balancing it with other rights and freedoms. It defines the boundaries of when the right may be exercised and when it may not be applicable. Accordingly, it becomes possible either to implement conflicting rights and concepts concurrently or, where necessary, to allow one right to yield to another.

At this point, it is first necessary to address which types of information should be removed in connection with the exercise of the right to be forgotten. Does the data subject's right to be forgotten imply that the relevant personal data must be removed from all platforms? Or does it merely restrict access to personal data based on certain circumstances or specific search queries? It must first be noted that this is a debate primarily relevant in the context of the digital environment. In cases where the right to be forgotten is exercised with respect to personal data in a physical medium, the only available solution would be the removal—or in other words, the destruction—of the material (such as newspapers, magazines, books, etc.) in which the personal data is contained.

However, the situation differs in the digital environment: The search terms used in search engines, the results returned, and the presence of the personal data in various formats and platforms all come into play. In fact, the risk associated with personal data in the digital environment stems precisely from this. Once personal data enters the digital sphere by any means, it can be used for a variety of purposes and disseminated across an extremely broad domain within seconds.

There are views asserting that the right to be forgotten does not in fact require the deletion or destruction of the personal data concerned, but rather its removal from search results in relation to specific queries. According to this perspective, the so-called “right to be forgotten” under EU law merely requires the deletion of information from search engines and does not necessitate its complete removal by the content provider. As a result, the relevant websites technically remain accessible, but they are no longer indexed in search engine results. In this sense, the rights to freedom of expression and privacy allow for the establishment of a relative balance.¹⁵²

Indeed, this was also the case in the Court of Justice’s Google judgment. Google noted that the decision was interpreted to mean that, in exercising the right to be forgotten, the personal data in question should not appear in the results of searches conducted using the data subject’s name. Accordingly, the data requested to be “forgotten” remains existent and accessible but does not appear before users in response to specific search queries.

This situation has been criticized on the grounds that it does not result in genuine forgetting. Indeed, it is impossible to speak of actual forgetting in a case where information does not appear only in specific searches —such as those using the data subject’s name— but remains accessible through other types of searches. While this approach may be somewhat effective in limiting the dissemination and accessibility of the information, it remains highly difficult for the right to be forgotten to fully achieve its purpose if the information in question can still be accessed through alternative means. Nevertheless, the necessity of maintaining internet freedom and balancing this right with other conflicting rights and freedoms requires such a limitation.

Therefore, in addition to defining the right to be forgotten and securing it through legal regulations, determining its scope in this way is important for establishing a balance where it conflicts with other rights and concepts.

¹⁵² **Woodrow Hartzog**, *Privacy’s Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press, Cambridge, 2018, 80.

b. Privacy by Design Standards

At this point, privacy by design standards are considered a solution not only for ensuring information security but also for implementing and improving laws and policies regarding personal data. For instance, within this framework falls the right to be forgotten, which—pursuant to the judgment of the Court of Justice—entails the removal by search engines of data that is “inadequate, irrelevant, no longer necessary, or excessive” from indexed search results.¹⁵³ However, there are still ongoing debates concerning the implementation of this right. Among the most prominent issues are the uncertainty in the decision-making process regarding how requests submitted by individuals should be handled, and the actual process of removing links from the platforms where they appear. For example, search engines such as Google have found themselves in a difficult position due to their obligations to ensure fairness, to comply with legal procedures, and to maintain transparency simultaneously.¹⁵⁴

Rigo Wenning, legal counsel to the World Wide Web Consortium (W3C)—which develops standards and guidelines to help everyone build a web based on principles of accessibility, internationalization, privacy, and security—has proposed the standardization of the web protocol known as “robots.txt.”¹⁵⁵ The robots.txt file is a simple text file placed within the file structure of a website, which sends a signal to the search engine indicating a request to avoid indexing and searching that content. All major search engines, including Bing, DuckDuckGo, and Google, comply with the robots.txt protocol. Wenning has proposed that the protocol be standardized to include a tagging function that would instruct search engines to ignore certain websites specifically for search queries using tagged terms (such as a person’s name). In other words, content marked with a specific tag —such as “Bill” and “William” under the tag “Will”— would appear in search results only if that specific name is queried. This type of standardization would make it possible to implement the right to be forgotten, so long as search engines like Google operate in compliance with the robots.txt protocol. Of course, such a solution would inevitably have its own set of problems.

c. Public Interest

In balancing the right to be forgotten with the rights and concepts it conflicts with; the criterion of public interest constitutes the most tangible and

¹⁵³ **Alan Travis/Charles Arthur**, “EU Court Backs ‘Right to Be Forgotten’: Google Must Amend Results on Request, 2014, <https://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results>.

¹⁵⁴ **Hartzog**, 165, 166.

¹⁵⁵ <https://www.youtube.com/watch?v=7ULzrDTzrXU>, 06.03.2024.

easily distinguishable standard. This criterion becomes particularly prominent in relation to the concept of historicity and the freedom of expression. Accordingly, in cases where a conflict arises between two interests, the interest of the public must prevail over individual protection.

As previously noted, the concepts of the right to privacy, the protection of personal data, and the right to be forgotten —although serving the public good due to their connection with human rights— are essentially related to personal integrity and aim to ensure individual protection and safeguards. By contrast, freedom of expression —especially in its dimensions of providing and accessing information— adopts a more collective and public-oriented perspective.

It must be noted that the concept of public interest is the most significant criterion in determining the limits of the right to be forgotten; therefore, its definition and its relationship with the right to be forgotten must be clearly articulated. Nevertheless, ECtHR has yet to provide a definitive assessment of the notion of public interest in cases involving a conflict between freedom of expression and the right to be forgotten under Article 8 of the Convention. That said, the ECtHR did express an opinion on this matter —at least in the context of the media— in its judgment in *Caroline von Hannover v. Germany*. The case concerned Caroline von Hannover’s claim for respect for her private life after taking legal action against photographers who had captured images depicting private activities entirely separate from her public life. The Court emphasized that “the dissemination of information must be limited to matters of public interest and must not extend to disclosing every personal and private detail concerning individuals, including public figures.”¹⁵⁶

The ECtHR’s judgment in *von Hannover v. Germany* clearly illustrates Europe’s approach to the right to privacy in the context of freedom of expression, and its method for balancing these rights when a conflict arises between an individual’s right to privacy and another person’s freedom of expression. The balance established between these fundamental rights reflects the role private law plays in regulating relationships between individuals. The claimant in this significant and noteworthy case was *Princess Caroline*, the eldest daughter of *Prince Rainier III of Monaco*. The case was brought before the ECtHR following claims that certain media outlets had taken photographs of the Princess in locations where she asserted a legitimate expectation of privacy. Princess Caroline argued that the publication of intimate photographs of her and her family in such settings by the media constituted a violation of her right to privacy under Article 8 of the ECHR. In the national proceedings, German courts reasoned that, given her position as a semi-public figure, the Princess’s right to

¹⁵⁶ *Caroline von Hannover. v. Germany*, 59320/00, 24.09.2004.

privacy was inherently reduced due to her social status and therefore allowed the publication of the photographs based on the principles of press and freedom of expression. In response, the Princess filed an application before the ECtHR against the German state, alleging that it had failed to fulfil its positive obligations under both the Constitution and the ECHR with regard to the regulation of mass media.¹⁵⁷

As a result of this application, the ECtHR found a violation on the part of Germany. Despite the Princess's status as a semi-public figure, the ECtHR reiterated that *"the concept of private life includes aspects relating to personal identity, such as a person's name or photograph"*. The Court held that *"private life must be taken to include a person's physical and psychological integrity"* and therefore interpreted Article 8 *"as protecting the right to personal development without external interference in an individual's relationships with others"*. This led the Court to conclude that¹⁵⁸ *"even in a public context, there exists a sphere of interaction with others which may fall within the scope of 'private life'"*.¹⁵⁹

In reaching this conclusion, the Court acknowledged that freedom of expression, as guaranteed under Article 10 of the Convention, must be balanced against the right to respect for private life.¹⁶⁰ The Court considered the publication of the photographs to be a violation of the Princess's right to privacy, as *"despite the applicant being known to the public, it could not be accepted that the published photographs contributed to any debate of general interest to society."*¹⁶¹ It must be remembered that this judgment rendered against the state, in fact, concerns a seemingly simple tort conflict involving a private individual, but *"due to its constitutional dimension,"* it was treated as a matter of public law. In the European approach, fundamental rights and freedoms do not merely protect the individual against violations by the state; they also oblige the state to take sufficient and positive measures to safeguard individuals against rights violations committed by other individuals. As a result, the Caroline von Hannover judgment constitutes a decision in which the allegation of a violation of the right to privacy was effectively analyzed through the lens of an individual right, rather than by restricting the right to privacy from the perspective of public

¹⁵⁷ Werro, 5, 6.

¹⁵⁸ Werro, 6.

¹⁵⁹ Caroline von Hannover. v. Germany, § 18-42.

¹⁶⁰ Caroline von Hannover. v. Germany, § 58.

¹⁶¹ Caroline von Hannover v. Germany, § 65.

law.¹⁶² Therefore, it is a significant ruling in terms of both the protection of personal data and the right to be forgotten.

As a result, whether the right to be forgotten may be exercised will largely depend on the relevance of the information to the public. In this regard, particular attention must be paid to the nature of the information, the status of the data subject, and whether the information remains of public interest in light of the time that has elapsed.

d. The Passage of Time as a Criterion

The time elapsed between the date on which the information subject to the right to be forgotten was first published and the date on which the right is invoked is of significance in terms of balancing the relevant rights. It should be noted that the element of time generally favours the application of the right to be forgotten. Indeed, the longer the period that has passed since the initial publication of personal information, the weaker its connection becomes with the rights and freedoms that conflict with the right to be forgotten.

On a temporal scale, the further back the origin of the information goes, the more likely it is that personal interests will outweigh and prevail over the public interest. Accordingly, starting from the general right to personality and extending to the specific right to be forgotten, both the direct and indirect implications of this right are examined; certain key data protection concepts are considered in light of the real-world application of this new and fundamental right; and the possible legal and technological limitations of the right are also taken into account.¹⁶³

In conclusion, concerns for privacy may justify the restriction of access to certain facts and the disclosure of previously publicized information, particularly where such information no longer carries news value. However, if the information remains necessary in terms of public interest, the right to be forgotten cannot be exercised.

D. Distinction Between the Right to Be Forgotten and the Right to Erasure

The fact that the right to be forgotten involves a request for the deletion of information relating to the data subject has led to its being considered alongside the right to erasure. Indeed, these two rights are often used interchangeably, based on the assumption that they share the same purpose and function. Moreover, there are cases in which critics of the right to be forgotten —on the

¹⁶² Werro, 6.

¹⁶³ Weber, 121.

grounds discussed above— express a more favourable view toward the right to erasure.

Whether this is merely a matter of terminological confusion or whether it reflects substantive differences is one of the debated aspects of the right to be forgotten. Initially, especially due to the GDPR addressing the matter within the scope of the right to erasure, it was assumed that the right to be forgotten served the same purpose and had the same scope as the right to erasure. However, over time, this view has been challenged and replaced by a debate as to whether “being forgotten” and “erasure” in fact refer to different concepts. Under this heading, it will be attempted to clarify this debate.

In our opinion, the right to erasure should not be equated with the right to be forgotten. Although both rights pertain to personal data and involve similar operations on data when exercised, the origins and underlying philosophies of these rights are entirely different.

It should be noted that this distinction is particularly emphasized by those who oppose the recognition of the right to be forgotten but support the right to erasure. According to this view, the right to be forgotten is concerned with rewriting history or censorship, whereas the right to erasure is about imposing more effective and stricter controls and limitations on the state, and about preventing the commercial retention of more data than necessary. Therefore, defining the latter as “forgetting” may be misleading, as erasure is not about forgetting—it is about control.¹⁶⁴

This view acknowledges that invoking the right to be forgotten may be appealing in certain respects yet argues that it becomes secondary when evaluated against the rights and concepts it conflicts with. Indeed, while the right to be forgotten may lead to a rejection of societal discourse and ultimately foster a non-democratic environment, the right to erasure can serve on the contrary, as a means of support and protection in individuals’ interactions with society. Therefore, the threat that the right to be forgotten poses to free speech is quite evident, whereas a more limited and qualified right would not have the same effect. Moreover, the right to erasure would generally be subject to exceptions in circumstances that qualify as expressions of free speech. Accordingly, it would be difficult to conclude that the exercise of the right to erasure inherently entails a violation of freedom of expression.¹⁶⁵

It is also argued that the right to be forgotten interferes with free enterprise, imposes restrictions and limitations, and potentially entails a significant financial

¹⁶⁴ Bernal, 201.

¹⁶⁵ Bernal, 201, 202.

burden. While the same could be said for the right to erasure, it is stated that the right to erasure is more effective in balancing competing interests and introduces more appropriate and reasonable limitations. Accordingly, the default assumption should be that individuals are entitled to erase their own data.¹⁶⁶

We believe that the right to be forgotten should be recognized to the extent that it is balanced against the conflicting rights and freedoms discussed above; however, we also agree with the view that the right to erasure and the right to be forgotten should not be treated as the same right. Nonetheless, this is not because the right to erasure is “good” and the right to be forgotten is “bad,” but rather because the two rights are based on fundamentally different foundations.

As has been explained in detail above, it is clear that the right to be forgotten conflicts with fundamental rights and concepts that are also of great importance to society. However, the individual’s present-day need to forget and to be forgotten, coupled with the development of digital technologies and the resulting risks posed to personal data, clearly demonstrates the necessity of the right to be forgotten. Therefore, the first step must be to acknowledge the necessity of this right and the fact that this need cannot be fulfilled solely through the right to erasure; from there, efforts should be made to ensure the right to be forgotten is implemented in the most reasonable manner possible.

IV. Status of the Right to Be Forgotten in Turkish Law

A. The Approach of the Constitutional Court and the Court of Cassation

1. The Constitutional Court’s N.B.B. Decision

The discussion of the right to be forgotten within the context of Turkish national law is also relatively recent. The matter was addressed in detail for the first time in the Constitutional Court’s decision in the case of N.B.B., dated 3 March 2016.¹⁶⁷

a. Facts of the Case

In the online archive pages of a nationally circulated newspaper, a total of three news articles were published—two in 1998 and one in 1999—regarding an incident in which the applicant was sentenced to a judicial fine following criminal proceeding brought against him on allegations of drug use. The applicant, noting that the aforementioned newspaper continued to make these articles accessible via the archive section of its website, sent a formal notice to

¹⁶⁶ Bernal, 202.

¹⁶⁷ N.B.B., AYM. 2013/5653, 03.03.2016.

the relevant press organization requesting the removal of the online content. In the content of the notice, it was argued that the news articles published on the website damaged the applicant's honour and reputation, violated his privacy, and negatively affected his family, professional, and social life, despite not being a public figure. After failing to obtain a result from the content provider through the formal notice, the applicant subsequently filed a request with the Criminal Court of Peace (as of June 2014, transformed into the Criminal Judgeship of Peace following the amendments made to the Criminal Procedure Code under Law No. 6545), seeking an order to block access to the relevant news content. The Criminal Court of Peace first emphasized freedom of expression and freedom of the press by stating that the primary role of the press is to inform the public about news that is of public interest and societal concern, that is factual and up-to-date, and to encourage public reflection, criticism, commentary, and warnings. However, upon reviewing the specific circumstances of the case, the court found that the article had lost its currency, lacked newsworthiness, and no longer served any public interest by remaining accessible. The court concluded that, in its current form, the content constituted distressing and harmful information concerning the applicant's private life and, by allowing unrestricted access to this private information, amounted to a violation of personality rights. Consequently, the court upheld the applicant's request to block access to the content.

Upon appeal, the case was brought before the Criminal Court of First Instance, which overturned the decision to block access. As its reasoning, the court stated that the news articles in question did not contain any content that violated the applicant's honour or reputation, and that the archived news reflected the apparent factual reality at the time it was published. In addition, the court noted that although the article contained facts and opinions that may have disturbed the applicant, a journalist cannot be held responsible for those facts later being proven incorrect if there was no intent to violate rights at the time of publication. Following this, the data subject filed an individual application before the Constitutional Court, claiming a violation of the right to protect and develop one's moral integrity, and specifically the right to protection of personal reputation.¹⁶⁸

b. Judgment

The Court first examined the application in the context of the right to the protection of personal reputation. Accordingly, the right to protect and develop one's material and moral integrity, as set forth in Article 17 of the Constitution, also encompasses protection against attacks on an individual's personal honour

¹⁶⁸ N.B.B., § 10-15, § 67-73.

and reputation. In this respect, the state has both a negative obligation not to arbitrarily interfere with the individual's personal honour and reputation — which is a component of their moral integrity— and a positive obligation to prevent assaults by third parties.

Referring also to the case law of the ECtHR, the Court emphasized that the right to the protection of personal reputation is part of the right to respect for private life as protected under Article 8 of the ECHR.

In addition, the Court stated that in order for the right to the protection of personal reputation to be invoked in specific cases, the attack in question must reach a certain level of severity, must significantly impair the applicant's ability to enjoy the right to reputation, and must not arise foreseeably from the applicant's own actions. Nonetheless, the Court also noted that in cases of online attacks, the accessibility, widespread dissemination, and ease of storing and preserving news and opinions in the digital environment must be taken into account, and that news reports which did not exceed the required threshold of severity at the time of publication or which stemmed from the individual's own actions may still harm a person's honour and reputation if they remain accessible online for an extended period.

The Constitutional Court then established a connection between the right to the protection of honour and reputation and the right to the protection of personal data. The Court stated that in order for publications on the internet to be made available online and for a link to be established between the person and the news content, the individual's personal data must, as a matter of technical necessity, be processed into the digital environment. It further noted that, within the meaning of Law No. 5651, content providers are the parties who upload such personal data to the internet and thereby make news articles about individuals accessible through online newspaper archives. In this context, the relationship between the right to the protection of honour and reputation and personal data necessitates that online attacks on a person's honour and reputation be assessed in connection with the right to the protection of personal data.

The Court, referring to the concept of personal data, recalled that personal data may only be processed in cases prescribed by law or with the explicit consent of the individual. However, it stated that a news article published within the scope of the constitutionally defined freedom of expression and freedom of the press constitutes an exception to these limits. This is because news and opinions uploaded to the internet within the scope of freedom of expression and freedom of the press will often involve the use and processing of personal data. Nevertheless, due to the widespread use of the internet and the media's increasing reliance on this medium, easier access to news archives has created a digital environment that does not allow news concerning individuals to be

forgotten. On the other hand, the Court has previously held¹⁶⁹ that freedom of expression encompasses not only the right to disseminate opinions and ideas, but also the right to access news and opinions.¹⁷⁰

Referring also to the Google decision of the Court of Justice of the European Union, which was examined above, the Court stated that the rights to freedom of expression and freedom of the press, on the one hand, and the right to protection of honour and reputation, on the other, are fundamental rights and freedoms that require equal protection. Therefore, the necessity has arisen to re-establish the balance that has been disrupted between these two fundamental rights. According to the Court, in today's world where forgetting is difficult due to online journalism, it would only be possible to restore that balance in terms of honour and reputation by recognizing individuals' right to be forgotten.¹⁷¹

At this point, the Court specified the elements to be considered in determining the existence of the right to be forgotten in order for it to be protected against the freedom of the press and freedom of expression:¹⁷²

In this context, in order for an online news article to be removed from the Internet within the scope of the right to be forgotten, factors such as the content of the publication, the duration of its availability online, whether it has lost its topicality, whether it can be considered historical data, its contribution to the public interest (the social value of the news, its relevance for the future), whether the person mentioned in the news is a politician or a public figure, the subject matter of the news or article, and whether it involves factual statements or value judgments, as well as the public's interest in the relevant information, must be evaluated on a case-by-case basis."

In addition, the Court recalled its previous judgment¹⁷³ in which it recognized that an interference with internet access should be examined within the scope of freedom of expression, and by referring to the case-law of the ECtHR, stated that online news archives fall within the scope of freedom of expression and freedom of the press, and that the removal of such archived news would constitute an interference with press freedom.¹⁷⁴ However, the Court also emphasized that the press —and thus news in online archives— must comply

¹⁶⁹ Emin Aydın, 2013/2602, 23/1/2014, § 40; Kamuran Reşit Bekir, 2013/3614, 8/4/2015, § 34.

¹⁷⁰ N.B.B., § 61.

¹⁷¹ N.B.B., § 30-46.

¹⁷² N.B.B., § 50.

¹⁷³ Yaman Akdeniz ve diğerleri, B. No: 2014/3986, 2/4/2014; Youtube Llc Corporation Service Company ve diğerleri [GK], B. No: 2014/4705, 29.05.2014.

¹⁷⁴ N.B.B., § 56, 61.

with the restrictions laid down in Articles 26, 27, and 28 of the Constitution, including the protection of “the reputation or rights of others, or their private or family life”.¹⁷⁵

In this context, the Court first stated that the news reports regarding the criminal proceedings from 1998 and 1999 concerning the data subject had lost their timeliness, and that they no longer held news value from a public perspective nor possessed any significance that would shed light on the future. With regard to the content of the news, it also cannot be said that ensuring their easy accessibility online is necessary for historical, statistical, or scientific purposes. In this regard, the Court held that the easy accessibility on the internet of news articles about the applicant—who is not a political or public figure—harmed the applicant’s reputation from the perspective of public interest.¹⁷⁶

Additionally, according to the Court, the news reports concerning the applicant are of the kind that should be evaluated within the scope of the right to be forgotten. In this regard, taking into account the ease of access provided by the internet, it was concluded that access to the aforementioned news should be blocked in order to protect the applicant’s honour and reputation. For these reasons, the Court found that the rejection of the applicant’s request to block access constituted a violation of the applicant’s constitutional rights.¹⁷⁷

In conclusion, this judgment is highly significant as it explicitly recognizes the right to be forgotten by the Constitutional Court. The Court appears to have determined that the right to be forgotten emerges as a natural consequence of the fundamental aims and duties of the state, the inviolability of the person, the right to protect one’s material and spiritual integrity, the right to privacy, and the right to request the protection of personal data. Within this framework, it is observed that the Constitutional Court seeks to establish a fair balance between freedom of expression and of the press, and the individual’s right to be forgotten. In this regard, the state bears responsibility to offer individuals the opportunity to “start a new chapter” by preventing others from learning about their past experiences. Accordingly, it is understood from the judgment that a positive obligation is imposed on the state to safeguard the right to be forgotten.

2. The Constitutional Court’s Fatih Saraman Decision

Another decision related to the right to be forgotten is the Constitutional Court’s decision in the case of *Fatih Saraman*, dated 27 February 2019.¹⁷⁸

¹⁷⁵ N.B.B., § 64.

¹⁷⁶ N.B.B., § 72, 73.

¹⁷⁷ N.B.B., § 74.

¹⁷⁸ Fatih Saraman, AYM. 2014/7256, 27.02.2019.

a. Facts of the Case

In the case subject to the application, the applicant committed the crime of theft while under the age of 18 and was convicted of this offense. After turning 18, he applied for the recruitment exam for correctional officers and passed the exam successfully. However, during the security investigation conducted prior to employment, his conviction from before the age of 18 was cited as the reason for not appointing him. Subsequently, the applicant exhausted all legal remedies and filed an individual application before the Constitutional Court, arguing that criminal archive records from before the age of 18 should not be taken into consideration in public employment decisions and should not be shared with any institution or individual other than judicial authorities.

b. Judgment

Although the Court examined all relevant legislation, particularly Article 20 of the Constitution and Law No. 6698, it primarily based its decision on the violation of Article 20 of the Constitution, concluding that there had been a breach of the right to respect for private life. Among the normative foundations of this decision are, inter alia, Article 53(4) of the Turkish Penal Code (TPC) and Article 10(3) of the Criminal Records Law No. 5352. According to TPC Article 53, although a person convicted of a crime may be deprived of certain rights, such a decision cannot be issued for individuals who committed the offense while under the age of 18 with respect to eligibility for public office or candidacy. According to Article 10(3) of the Criminal Records Law, *“Judicial records and archive records concerning individuals under the age of eighteen may only be requested by public prosecutors, judges, or courts for the purposes of investigation and prosecution.”* Despite these provisions, the criminal record of the applicant—who was under 18 at the time of the offense—was disclosed to another authority, and although such a restriction is not prescribed under Article 53 of the Penal Code and no such decision had been made, the applicant was denied appointment to public office.

The administration based its decision on the provisions of Law No. 4045, titled “Law on Security Investigations, the Reinstatement of Rights of Public Officials Who Have Been Dismissed for Certain Reasons or Denied Appointment to Public Office, and the Amendment of Martial Law No. 1402.” Security investigations and background checks for personnel to be employed in certain public positions are conducted pursuant to Law No. 4045. However, Article 48 of the Civil Servants Law No. 657 was amended by Decree-Law No. 676 dated 03.10.2016, and subsequently approved by Law No. 7070. As a result of this amendment, it was stipulated that a security investigation and background check must be conducted for all individuals to be appointed to civil service

positions, thereby establishing such investigation and research as a general prerequisite for public employment.¹⁷⁹

The Court stated that Law No. 4045 does not contain any provisions regarding the duration and manner of processing personal data, and further noted that there are ambiguities in the regulation issued to implement this Law. It then addressed the right to be forgotten as follows:

*“It is observed that Law No. 4045 does not contain any provisions regarding which information and documents will be the subject of the security investigation and archive research, from where such information will be obtained, in what manner and for how long it will be stored, whether individuals will have the opportunity to object to such information, whether it will be possible to delete the information after a certain period, or what procedure will be followed for deletion; nor does it contain any provision regarding the identification of public personnel with classified clearance or professional groups, the procedures and principles of the security investigation and archive research, or the competent authorities to carry out these procedures. Moreover, it is understood that the law does not refer to Law No. 5352—which is the primary law to be considered and applied in relation to finalized criminal convictions—and that it lacks any provisions protecting individuals against arbitrariness. Likewise, the Regulation on Security Investigation and Archive Research does not regulate the duration of data retention, whether deletion after a certain period is possible, or the procedure to be followed for deletion, or whether individuals have the opportunity to object to such information, and it is understood that it lacks provisions to ensure the protection of the right to respect for private life.”*¹⁸⁰

The Court also implicitly acknowledged the existence of the right to be forgotten through similar statements and, based on this, identified the unlawfulness in the case at hand, particularly in relation to the regulation that was applied:

“Moreover, the Regulation stipulates that the information and documents resulting from the investigation and research shall be kept indefinitely in the security files of the person concerned, and that information regarding those with adverse findings in the security investigation and archive research shall be mutually shared

¹⁷⁹ Fatih Saraman, § 71-73.

¹⁸⁰ Fatih Saraman, § 83.

between the National Intelligence Organization (MİT) and the General Directorate of Security. It is observed that individuals are neither provided with the opportunity to object to such information, nor is any provision made for its deletion after a certain period of time. In this context, it is understood that the security investigation and archive research are not subject to objective, foreseeable, and pre-determined safeguards and procedures, but rather are conducted entirely based on the instructions of the competent authorities, thus creating a situation prone to arbitrariness.”¹⁸¹

According to the Court, the provisions of Law No. 4045 fail to properly define the fundamental principles, framework, and essential elements of the matter concerning the restriction of fundamental rights and freedoms. The Court stated that the Law in question does not include clear and detailed rules that would ensure sufficient safeguards against arbitrary practices and abuse of authority by those subject to its implementation. Therefore, the regulation forming the basis of the interference in the present application does not fulfil the requirement of legality.¹⁸² As a result, the Court held that Article 20 of the Constitution had been violated.

Although the Court based its judgment on the principle of legality, the actual issue that should have been explicitly addressed was the violation of the “right to be forgotten.” This is because Article 53(4) of the Turkish Penal Code and Article 10(3) of the Criminal Records Law specifically regulate the right to be forgotten in relation to minors. Accordingly, these provisions were enacted to ensure that children are not affected for the rest of their lives by offenses committed before reaching the age of majority, when their cognitive and volitional capacities are not fully developed, and so that such offenses do not hinder their right to education and employment. The practical application of this right granted to children lies in ensuring that special categories of personal data are not disclosed to or processed by parties other than the relevant authorities.

However, in the case that is the subject of the application, personal data were both shared with unauthorized authorities and processed, thereby clearly violating the law and infringing the individual’s right to the protection of personal data, the right to work, and the right to be forgotten. Therefore, the Court’s decision is appropriate and a progressive step, underlining that no matter the subject, no action can be taken in violation of normative regulations and that the right to be forgotten must be fully enforced.

¹⁸¹ Fatih Saraman, § 89.

¹⁸² Fatih Saraman, § 90.

This decision also constitutes a continuation of the Constitutional Court's stance in favour of recognizing the right to be forgotten, as adopted in its N.B.B. ruling. Therefore, it is a favourable decision in this respect as well.

B. The Approach of the Court of Cassation

1. Decision of the General Assembly of Civil Chambers of the Court of Cassation dated 17.06.2015

The allegation of violation of the right to be forgotten has also been the subject of compensation claims based on an infringement of personal rights. It is necessary to mention the decision rendered by the Court of Cassation, as it is the first time the right to be forgotten has been addressed and defined in Turkish law.

The decision given by the General Assembly of Civil Chambers of the Court of Cassation (YHGK)¹⁸³ concerns a compensation claim based on an alleged infringement of personal rights, resulting from the publication of a criminal judgment concerning the data subject, without anonymization, in a scientific book.

In the case at hand, the data subject stated that a judicial decision included in the book mentioned she was the victim of the offense of repeated sexual assault, perpetrated by abusing the influence of a public office or service relationship.

As a result of the trial, the defendant, a public official, was convicted. Upon appeal, the judgment was upheld in 2009. During both the investigation and the trial, the victim (the data subject) explicitly described how the sexual assault occurred, and these statements were included in the text of the judgment. The inclusion of this decision, which fully narrates the incident, in a book published in April 2010—four years after the incident and without the victim's consent— was made the subject of a compensation claim by the data subject. The data subject seeks, through the right to be forgotten, to move beyond the unfortunate incident in her past and shape her future freely—in other words, to have the opportunity to start a new chapter in her life.

The General Assembly of Civil Chambers (YHGK) approached the issue as a conflict between the protection of personal data and personal rights arising from the right to be forgotten, and the limits of the freedoms of science and art. According to YHGK, the resolution of the issue requires establishing a fair balance between freedom of science and art and the individual's fundamental

¹⁸³ YHGK, 17.06.2015, E. 2014/4-56, K. 2015/1679.

rights. YHGK first determined the scope of the concept of personal data and then set out the underlying purposes and principles of personal data protection:

“The protection of personal data is closely related to human rights. This is because the disclosure of personal data may, first and foremost, violate the right to privacy and may also harm several other related rights.

There is no explicit provision in the ECHR regarding personal data. However, the Court, through its rulings, has established the content of the concept of personal data. It must be stated immediately that it is not possible to numerically limit what constitutes personal data. Nevertheless, considering case law and academic publications, personal data can be understood to include information that reveals a person’s identity, makes a person identifiable, or characterizes them—such as their identity, economic and digital information, nationality, beliefs, race, political opinions, philosophical beliefs, religion, sect or other beliefs, association, foundation and union memberships, health data, photographs, fingerprints, health records, text messages, contact lists, and writings, photos, audio or video recordings shared on social networking sites.

In our time, the protection of personal data is gaining increasing importance in parallel with the development of the concept of human rights and the growing awareness of their protection. The main purpose of the right to the protection of personal data is to safeguard individuals by ensuring the confidentiality of their private life. The right to the protection of personal data, which has become an increasingly important issue in the information society, appears as a requirement for individuals to regulate their own lives with free will in a democratic state governed by the rule of law. Moreover, the ability of an individual to freely develop their personality, the protection of that personality, and the formation of a social order composed of free individuals is only possible through the protection of their right to personal data. As stated above, this right is explicitly regulated in Article 20(2) of the Turkish Constitution.”

Afterward, the YHGK addressed the right to be forgotten by associating it with the right to the protection of personal data yet treating it as an independent right. In this respect, according to the YHGK, the right to be forgotten essentially forms the framework of the right to the protection of personal data, particularly with regard to compliance with the principles of proportionality and reasonable time in storing or retaining personal data. Accordingly, both rights are fundamentally based on enabling individuals to freely control their personal data,

to make plans for the future without being hindered by their past, and to prevent the use of their personal data against them.

Subsequently, the YHGK also included in its decision the first definition of the right to be forgotten in Turkish national law:

“The right to be forgotten can be defined as the right to request the deletion and prevention of the dissemination of personal data related to past negative events stored in digital memory, which one does not wish others to know, unless there is an overriding public interest.”

In this context, the content of the right to be forgotten is set forth in the decision through a twofold analysis: On the one hand, by granting the data subject the right to “control their past” and the right to “request the deletion of certain elements from their past and not to be remembered,” and on the other hand, by imposing an obligation on third parties not to use or recall certain information about the person. In its decision, the YHGK also concluded that although there are opinions suggesting that the scope of the right to be forgotten is limited to digital data, considering the characteristics of this right and its connection with human rights, it must be recognized not only for personal data in digital environments but also for personal data that is kept in places easily accessible by the public.

The question of whether the right could be assessed under Article 8 of the ECHR, which protects the right to respect for private life, was also addressed in the decision. The ruling included the view that the “right to privacy” protected under the right to respect for private life also encompasses an individual’s legal interest in controlling information about themselves. Accordingly, the data subject has a legal interest in ensuring that their data is not disclosed, disseminated, or accessed by others without their consent—in other words, that their personal data remains private.

In the specific case at hand, the YHGK determined that there were no special reasons indicating an overriding public interest—such as the data playing a significant role in public life or attracting intense public attention. Therefore, it concluded that the personal data should not have been included explicitly in the academic publication and upheld the data subject's claim for compensation. On the other hand, the minority opinion held that there was no need to anonymize names mentioned in court decisions, emphasizing that court proceedings are, except in special cases, conducted publicly and that judgments are pronounced openly. Therefore, they argued that there was no violation of the right to privacy.

In this context, the decision is considered a highly positive development in that it recognizes the right to be forgotten as an independent right and provides its definition for the first time by the courts. Moreover, the decision is significant

in that the failure to fulfil the right to be forgotten can be regarded as a violation of personal rights and may give rise to claims for compensation.

2. Decision of the Criminal General Assembly of the Court of Cassation dated 30.10.2018

One of the significant rulings in which the right to be forgotten was discussed alongside freedom of expression and freedom of the press is a decision by the Criminal General Assembly of the Court of Cassation regarding a newspaper article.¹⁸⁴ The case concerned a complaint made by an individual who had been convicted under Article 765 of the former Turkish Penal Code for the offense of ‘detaining with lustful intent’ and who objected to a column published in a newspaper 22 years after the incident. The complainant stated that *“the incident took place in 1991, that he had been prosecuted and sentenced, that the sentence had been suspended, that he started working in 1998 as an administrator at the Provincial Directorate of Youth Services and Sports in Osmaniye, and that the publication of such a report 22 years later was intended to damage his reputation, that there was no public interest in the article, and that the report caused serious problems within his family.”*

Considering that the incident is directly related to freedom of expression and freedom of the press, the Criminal General Assembly of the Court of Cassation (YCGK) first concluded that these aspects should be evaluated within the framework of national and international regulations, and then emphasized that the elements of the right to report news, criticism, and the right to be forgotten—which has taken root in our legal system through case law—as well as the elements of the offense of defamation should be examined.

Within this framework, the review first referred to international and national regulations on freedom of expression, emphasizing that freedom of expression is an indispensable requirement of democracy, the basis of many rights and freedoms, as well as the source of personal and societal development, and therefore it is guaranteed in the broadest sense. Subsequently, freedom of the press was addressed, along with its exceptions. According to the YCGK:

“In today’s liberal democracies, except for exceptions, a wide range of expression is protected, and by being evaluated within the scope of freedom of expression, individuals are allowed to benefit from the rights provided by this freedom to the fullest extent.”

On the other hand, the YCGK also acknowledges that a balance must be established between the freedoms of expressing, disseminating thoughts, freedom of expression and of the press, and the protection of individuals’ honour

¹⁸⁴ YCGK, 30.10.2018, E. 2016/18-1169, K. 2018/490.

and reputation. It holds that, while the use of the internet requires that the aforementioned fundamental rights and freedoms be protected in the digital environment as well, it also brings about interventions in these rights and freedoms in view of the risks posed to the right to privacy, honour and reputation, and the protection and development of material and moral integrity. The YCGK states that due to the effective use of the internet by the press, the balance—which should be equally maintained between freedom of expression and press and the individual’s dignity and reputation—has been disrupted in favour of press freedom, and that the prevention of this disruption is only possible through recognition of the right to be forgotten.

In light of all these considerations, the YCGK concluded that in the concrete case, due to certain elements involved, the right to be forgotten and the individual’s honour, dignity, and reputation should prevail.

“In light of the overall structure of the article and the manner in which the expressions were used; the fact that the conviction against the complainant—which constitutes the basis of the article—pertained to an incident that occurred approximately twenty years ago and, according to the provisions governing criminal record registers, is to be regarded as legally non-existent; that the complainant has the right to request protective measures within the scope of the right to be forgotten with respect to the said incident; that the complainant, by virtue of the nature of the public office he held, was not in a position that would draw special attention from the public, nor was he involved in a political, media-related, or similar role; that the nature of the complainant’s public duty did not significantly change in a way that contradicted the content of the article; and that the journalist, despite personally possessing and having the opportunity to review and evaluate the previous conviction judgment against the complainant—which concerned the offense of abduction for lustful purposes regulated under Article 430/2 of the former Turkish Criminal Code No. 765—misrepresented it as a different and more serious offense of sexual abuse; when all these factors are considered together, it cannot be said that the article had any current news value or that there was a public interest in knowing and discussing this matter. It is thus understood that the defendant’s conduct created a real danger of undermining the public trust that must exist toward the complainant, who is a public official. Accordingly, the expressions used in the article must be considered as having been of a nature that offended the honour, dignity, and reputation of the subject.”

This decision rendered by the YCGK is extremely important in terms of specifying which elements are to be considered in the application of the right to be forgotten. Accordingly, the criteria evaluated by the YCGK are as follows:

- The passage of time since the incident: One of the most important elements in the application of the right to be forgotten is the time elapsed since the incident. The Criminal General Assembly of the Court of Cassation (YCGK) emphasized that 22 years had passed since the event.
- Characteristics of the person invoking the right to be forgotten: The YCGK noted that, due to the nature of the public office held by the complainant, the individual was not in a position of particular public interest, such as political, media-related, or similar status.
- Currency of the content subject to the right to be forgotten: According to the YCGK, the news item did not have current relevance.
- Accuracy of the content subject to the right to be forgotten: Although the right to be forgotten primarily concerns true events, the YCGK emphasized the importance of the fact that the event was “portrayed differently and in a more severe manner” than it actually was. In such cases, the likelihood of the right to be forgotten being applied increases.
- Public interest: The YCGK concluded that there was no public benefit in learning about or discussing the issue. On the other hand, the news in question posed a real danger to the public trust that should be placed in the complainant, who is a public official.

C. The Approach of the Personal Data Protection Board

Due to the fact that the right to be forgotten is directly related to the right to the protection of personal data, how the Personal Data Protection Board (“KVKK”) approaches the matter is of utmost importance. The KVKK addressed the right to be forgotten for the first time in a decision issued in 2020, and since then has published numerous regulations on the subject.

1. The Decision of the Personal Data Protection Board Dated 23.06.2020 and Numbered 2020/482

The KVKK, upon receiving various applications that included requests for “the deletion of names and surnames mentioned in news articles published on websites or the removal of such news within the scope of Law No. 6698” and for “technical arrangements preventing the indexing of such newspaper archives

by search engines,” felt the need to evaluate the right to be forgotten for the first time.¹⁸⁵

In its assessment, the Board sought to determine the scope of the matter by referring to relevant national and international regulations and court rulings. According to KVKK, although the concept of the right to be forgotten is not explicitly mentioned in our legislation, it is evident that there are legal mechanisms in place to ensure this right.

Therefore, there remains no doubt that KVKK acknowledges the right to be forgotten. Following this, KVKK made an evaluation regarding how future applications within the scope of the right to be forgotten would be handled. As a result of this evaluation, the Board reached the following conclusions:

- Search engines are data controllers, and the activities carried out by search engines constitute personal data processing activities.
- Although the right to be forgotten is an overarching concept, applications related to this matter are evaluated within the scope of Article 20/3 of the Constitution, Articles 4, 7, and 11 of Law No. 6698, and Article 8 of the Regulation on the Deletion, Destruction, or Anonymization of Personal Data.
- Data subjects must first apply to the data controller search engines regarding their requests for the removal of search results from the index. If these applications are rejected or left unanswered, they may file a complaint with the Board. In such cases, data subjects may also directly initiate legal proceedings.
- When evaluating such requests, a balance test will be conducted between “the fundamental rights and freedoms of the data subject and the public’s interest in accessing the relevant information.” However, additional criteria may also be considered depending on the specific circumstances of each case.

The KVKK has published a Q&A-style document regarding the criteria to be considered in evaluations within the scope of the right to be forgotten; all of the criteria included in that document are also covered in our study.¹⁸⁶

In addition, the “*Public Announcement on Requests for the Removal of Results from Search Engine Indexes Based on Searches Using Individuals*”

¹⁸⁵ KVKK, 23.06.2020 tarihli ve 2020/482 sayılı Karar Özeti, www.kvkk.gov.tr. (Summary of the Decision No. 2020/482 dated 23.06.2020 of the Personal Data Protection Authority)

¹⁸⁶ KVKK, Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına İlişkin Değerlendirmede Dikkate Alınacak Kriterler, www.kvkk.gov.tr (Criteria to Be Considered in the Evaluation Regarding the Removal of Search Results Indexed by Search Engines Based on Individuals' Name and Surname – Published by the Personal Data Protection Authority)

Names and Surnames”, which reflects the decision and the conclusions reached by the KVKK, was published on July 17, 2020, in parallel with the decision summary mentioned above.¹⁸⁷ This announcement additionally stated that the procedures and principles set out in the decision would be communicated to search engine operators and that necessary actions would be taken to ensure the implementation of the right to be forgotten.

2. Decision of the Personal Data Protection Authority (KVKK) dated 08.12.2020 and numbered 2020/927

This decision of the KVKK is extremely important in that the criteria stated in the previous decision were evaluated in the context of a concrete case.¹⁸⁸ The case in question concerns the publication of a news article about an investigation initiated against a university faculty member. The applicant stated that the removal request submitted to the search engine had been unsuccessful and that the news article in question had negatively affected their life and therefore requested that the content be subject to technical arrangements so as not to be indexed by the search engine.

The criteria examined by the KVKK in relation to this application and the circumstances of the specific case are as follows:

Question	Circumstance in the specific case
Is the content subject to the application accurate?	Yes
What is the content about?	It is related to the data subject's professional life, and the person is still employed in the same position.
Does the content include any special categories of personal data?	No

¹⁸⁷ KVKK, Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler Hakkında Kamuoyu Duyurusu, www.kvkk.gov.tr

¹⁸⁸ KVKK, 08.12.2020 tarihli ve 2020/927 sayılı Karar Özeti, www.kvkk.gov.tr. Summary of the Decision of the Personal Data Protection Authority (KVKK) dated 08.12.2020 and numbered 2020/927

Is the content up to date?	Yes
Is there a legal obligation for the publication of the content?	No
Was the content published by the data subject?	No
Is the content related to a criminal offense?	No

The KVKK, considering all these aspects, concluded that the data controller's decision not to remove the content was appropriate.

3. Decision No. 2020/414 of the Turkish Personal Data Protection Authority (KVKK), dated 22.05.2020

In the case subject to this decision of the KVKK, the issue concerned the publication on a newspaper's website of a judgment rendered within the scope of a criminal prosecution against the data subject.¹⁸⁹ In the application submitted by the data subject's attorney, it was stated that the offense in question dated back to 2009, the imposed sentence had been fully executed, and the publication of the news article had negatively affected the data subject's professional and family life.

The newspaper that published the article, on the other hand, presented a defense precisely within the framework of the rights and principles that conflict with the right to be forgotten. It argued that: (i) pursuant to Article 28(1)(c) of the Law on the Protection of Personal Data, the processing of personal data within the scope of freedom of expression constitutes a justification for lawfulness; (ii) under Article 26 of the Constitution, receiving and imparting information is considered a component of freedom of expression; (iii) the news in question was written within the scope of the public's right to receive information; (iv) press and media freedom is accepted as a fourth power following the legislative, executive, and judicial branches; (v) if such news is removed solely on the grounds that it is disturbing to the data subject and without regard to public interest, it would pose a threat to the functionality of the media; (vi) there was no disclosure of confidential information by the parties; and (vii)

¹⁸⁹ KVKK, 22.05.2020 tarihli ve 2020/414 sayılı Karar Özeti, www.kvkk.gov.tr. Summary of the Decision of the Personal Data Protection Authority (KVKK) dated 22.05.2020 and numbered 2020/414

regarding the removal of publications, the procedures set out in Law No. 5651 could be pursued.

In its examination of the specific case, the KVKK concluded that the news article served the public interest and that, in light of the conflicting rights, freedom of expression prevailed over personal rights. Accordingly, it determined that no action could be taken since the application fell within the scope of Article 28(1)(c) of Law No. 6698.

4. Decision of the Turkish Personal Data Protection Authority (KVKK) dated 10.11.2022 and numbered 2022/1201

In its most recent published decision on the matter, the KVKK accepted the application under the scope of the right to be forgotten and decided to instruct the data controller to ensure that the content subject to the application is de-indexed in a way that it can no longer be associated with the data subject's name and surname.¹⁹⁰ In the case at hand, the data subject submitted a request for removal on the grounds that a search of their name via a search engine led to a page of the Official Gazette, and requested that this page be taken down.

In its examination, the KVKK determined that the content subject to the application concerned a notification made to the data subject under the Notification Law. According to the Notification Law, the content in question is deemed to have been served within fifteen days of its publication in the Official Gazette. Therefore, first and foremost, the content subject to the application does not serve any public interest. Furthermore, more than twenty years have passed since the incident in question, rendering it outdated. Although the information in the content confirms, by a court decision, that the data subject was acquitted of the alleged crime, KVKK held that it could still lead to prejudice against the individual. Finally, the content in question is unrelated to journalistic activities. Considering all these factors together, the data subject's request to exercise the right to be forgotten was deemed justified.

With this decision, it can be concluded that the concepts the KVKK considers most significant in determining the legitimacy of a right to be forgotten request are public interest, timeliness, and freedom of the press.

V. The Right to Be Forgotten from the Data Controller's Perspective

Since the right to be forgotten involves, a request initiated by the data subject, there must necessarily be a party to whom this request is addressed and

¹⁹⁰ KVKK, 10.11.2022 tarihli ve 2022/1201 sayılı Karar Özeti, www.kvkk.gov.tr. Summary of the Decision of the Personal Data Protection Authority (KVKK) dated 10.11.2022 and numbered 2022/1201

who is responsible for fulfilling it. That party is, without a doubt, the data controller. While the data controller is recognized as having certain obligations within the scope of the right to be forgotten, the fact that this right is not explicitly regulated makes it difficult to clearly define those obligations. Although the right has been recognized particularly through court decisions and has been theoretically grounded to some extent, the absence of a clear legal provision means it is impossible to impose direct responsibility on the data controller.

However, the data subject's "*right to erasure/right to be forgotten*" is regulated under Article 17 of the GDPR, which clarifies what actions the data controller must take in response to a deletion request. As mentioned throughout this study and previously explained under a separate heading, the right to erasure and the right to be forgotten are not entirely synonymous. Therefore, although the responsibilities that may be imposed on data controllers will largely resemble each other, they will not be exactly the same.

Accordingly, in this section, we will attempt to outline the obligations of the data controller within the framework of the right to be forgotten by referring to Article 17 of the GDPR. Where relevant, we will also discuss initiatives taken by Google, as previously outlined above. Lastly, we will examine the potential obstacles a data controller may face when fulfilling such requests. In this way, we aim to clarify the meaning of the right to be forgotten from both the perspective of the data subject and that of the data controller.

A. The Data Controller's Duties Within the Scope of the Right to Be Forgotten

Article 17 of the GDPR, titled "*Right to erasure ('right to be forgotten')*", is the fundamental provision that explicitly includes the right to be forgotten. In this way, the GDPR addresses the right to erasure and the right to be forgotten as interchangeable concepts.

The inclusion of the term "*right to be forgotten*" in the Regulation was not easily achieved, even though it had been explicitly mentioned in the European Commission's press release in 2010. While the Commission advocated for the explicit reference to this right, the European Parliament preferred to use the term "right to erasure" as previously stated in Article 12 of Directive 95/46/EC. After prolonged negotiations, and once the Council of the European Union was convinced to accept the term, Article 17 of the Regulation came to regulate both the right to erasure and the right to be forgotten together.

Nevertheless, in its commentary on key issues of data protection law, the GDPR specifies that the right to be forgotten was introduced for the first time as an "addition" to the right to erasure. This point will be discussed in more detail

later. However, for the purpose of determining the obligations of the data controller within the scope of the right to be forgotten, it is necessary to examine Article 17.

Paragraph 1 of the Article sets out the data controller's obligation to erase personal data without undue delay where certain conditions are met: When the personal data are no longer necessary in relation to the purposes for which they were collected or processed; when the data subject withdraws consent and there is no other legal ground for the processing; when the data subject objects to the processing; when the personal data have been unlawfully processed; when the data must be erased for compliance with a legal obligation; or when the data have been collected in connection with the offer of information society services. It should be noted that this provision concerns the right to the protection of personal data and outlines the data controller's obligations under that right.

Paragraph 2, however, addresses situations where personal data have been "made public" and thus aligns more closely with the right to be forgotten. Indeed, in its explanation of key data protection concepts, the GDPR notes that the right to be forgotten is reflected in Paragraph 2 of Article 17. At this point, it briefly sets out what the data controller must do first under the right to erasure and then, additionally, under the right to be forgotten.

Accordingly, there is no specific definition or mandatory method prescribed for how personal data must be deleted. The only decisive factor is that, following the processing activity, it must no longer be possible to identify the personal data without disproportionate effort. In this regard, it is considered sufficient that the medium in which the data is stored is physically destroyed or that the data is permanently erased using specialized software. The same principle applies under Law No. 6698. Neither the Law itself nor the "Regulation on the Deletion, Destruction, or Anonymization of Personal Data",¹⁹¹ which entered into force after the Law, provides a specific description of how the data controller must carry out the deletion process. Although the choice is left to the discretion of the data controller, it is stated that the data controller must select the most appropriate method by taking into account the specific circumstances of the case.

With regard to the right to be forgotten, additional obligations have been introduced. Specifically, to strengthen the right to be forgotten in the online environment, if the data controller has made the personal data public and one of the grounds for erasure exists, the controller must take reasonable steps to inform

¹⁹¹ RG. 28.10.2017/30224.

other data processors about the request. In doing so, all copies of the personal data must be deleted.¹⁹²

Frankly, it cannot be said that the right to be forgotten introduces major changes beyond the obligations already established under the right to erasure. The main addition is that the data controller must inform other data processors and ensure the deletion of all copies. Since the obligation is limited to taking reasonable steps, it does not impose a substantial burden on the controller in terms of communication with other processors. Furthermore, it remains unclear whether the reasonableness of the steps to be taken will be assessed based on the subjective circumstances of the data controller or according to objective criteria.¹⁹³

Firstly, we believe that the explicit requirement for the deletion of copies aligns with the objectives of the right to be forgotten. Achieving this objective is only possible if the copies of the personal data—which the data subject no longer wishes to be remembered by or associated with—are also deleted. Otherwise, it would be impossible to speak of effective forgetting or the exercise of this right.

The obligation to delete copies in the context of the right to be forgotten should, a fortiori, apply to the right to erasure. In fact, while deletion of copies is arguably mandatory under the right to erasure, its necessity under the right to be forgotten remains open to debate. This is because, unlike erasure, the right to be forgotten does not necessarily entail the complete removal of personal data but rather seeks to limit its discoverability—especially via search engines. Nevertheless, the practical implementation of deleting copies poses significant challenges for both rights. In large organizations, the routine duplication of massive data sets is one of the main reasons for this difficulty. Not only is identifying and removing a single piece of data from among these copies technically complex, but it is also highly costly.

We anticipate that this issue will either require a new regulatory framework in the future or will evolve differently in practice. After all, in a digital world shaped by internet technologies and electronic devices, true forgetting may, in reality, be unattainable.

On the other hand, the GDPR imposes this obligation “where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data”; in other words, the GDPR limits this obligation to the cases specified in the first paragraph of the same article, which regulates the conditions under which personal data must be erased. Therefore, no additional

¹⁹² Recital 66, <https://gdpr-info.eu/recitals/no-66/>. 23.05.2020.

¹⁹³ **Paul Voigt/Axel von dem Bussche**, *The EU General Data Protection Regulation (GDPR)*, Springer, Heidelberg, 2017, 163.

circumstances are envisaged under which the right to be forgotten may arise. In our view, this indicates that the right to be forgotten is not treated as distinct from the right to personal data protection in terms of its elements, objectives, and the legal interest it protects. After all, the circumstances under which a right can be invoked are inherently linked to its elements and objectives. However, although the GDPR introduces additional obligations under the right to be forgotten beyond those under the right to erasure, the fact that the right to be forgotten is confined to situations where “personal data must be erased” narrows the scope and function of this right.

Of course, this should not be interpreted as requiring an overly broad scope for the right to be forgotten. As previously mentioned, such an approach could lead to serious conflicts with other fundamental rights and freedoms, such as freedom of expression and the right to access information. Nevertheless, we believe that it is necessary to identify the circumstances in which the right to be forgotten may arise in addition to the right to erasure, along with the foundations, purposes, and functions on which this right is based.

At this point, it is also important to refer to the initiatives of Google, the first entity to be placed under obligations to implement the right to be forgotten. The CJEU decision discussed above is significant in many respects: For the first time, a binding obligation was imposed to ensure the right to be forgotten, and this obligation was directed at a global company like Google. Particularly considering how many aspects of the issue remained unclear at the time, it was also challenging for Google to fully understand its obligations under the ruling. Indeed, Google acknowledged this and clearly stated that it had struggled to determine how to implement the decision. The ruling imposed considerable obligations, and the fact that it was followed by millions of requests clearly demonstrates its practical impact.

Nevertheless, opening a web form to the public for submitting such requests and publishing reports on the matter were important steps toward ensuring protection of the right. Furthermore, the inclusion of information on how the issue is addressed and clear explanations of how requests are assessed and resolved under the ruling is also noteworthy.

The establishment of an Advisory Council composed of experts by Google to properly implement its obligations under the ruling is a positive sign of its willingness to comply. However, this alone does not mean that Google has taken all possible measures. In fact, for a company of its size—whose core business is data processing—implementing all necessary measures inevitably takes time.

In conclusion, when exercising the right to erasure, the data controller should take the following points into consideration:

- The method and manner of executing the erasure process falls within the data controller's discretion.
- The data controller must determine the most reasonable option among the available alternatives.
- It should no longer be possible to identify the personal data without disproportionate effort.

With regard to the right to be forgotten, the following additional obligations apply:

- First, the data controller must inform all other data processors about the matter.
- In doing so, the data controller must ensure that all copies of the personal data subject to the right to be forgotten are deleted.
- The data controller must take all necessary and reasonable steps in both respects.
- In addition, the data controller must implement appropriate technical and organizational measures to enable recipients to erase the personal data in order to fulfil the right to be forgotten. In this context, a "Data Protection Management System" may be helpful, particularly for recording processing activities where appropriate.¹⁹⁴

B. Applicability of the Right to Be Forgotten and the Obstacle Created by HTTPS

In order for the right to be forgotten to be effectively protected, it is necessary not only for data controllers to fulfil their obligations, but also for court rulings—as the highest authority responsible for the implementation of the law—to be enforced, thereby ensuring that the law is put into practice. However, in the context of Türkiye, problems stemming from the HTTPS protocol constitute one of the major obstacles to the enforceability of the right to be forgotten.

As previously noted, the vast majority of the data subject to the right to be forgotten exists in digital form. Therefore, the enforceability of decisions related to this right depends on the deletion of the relevant data from digital platforms, in other words, technically blocking access to it. The rules governing the blocking of internet access and communication are regulated under Law No. 5651, titled the "Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications." According to Law No. 5651, there are four methods of access blocking: Blocking by domain name, by IP address, by content (URL), and by similar technical means. Except

¹⁹⁴ Voigt/von dem Bussche, 163.

for the cases listed under Article 8 of the Law, access blocking orders are carried out by the Union of Access Providers.

In cases where a violation of personal rights occurs online, there are two remedies available for the right-holder to request access blocking. The first is the notice-and-takedown method directed to the content provider, and the second is an application to the magistrates' court (sulh ceza hakimliđi). The magistrates' court must issue a ruling within 24 hours, and the content provider must respond to the application within the same timeframe.

HTTP (Hyper Text Transfer Protocol) is a communication protocol that establishes the rules for data transfer between clients and servers on the internet. It operates within a framework of specific rules that govern how communication and data exchange occur. When a request is made from a client to a server through a web browser, the server responds via various programs, thereby enabling internet browsing. HTTPS, on the other hand, is the secure version of HTTP, incorporating the SSL (Secure Socket Layer) protocol. In simpler terms, it is an enhanced, more secure form of HTTP. Normally, access to a website can be blocked by intervening in the transmission chain between the server and the browser. However, in cases where HTTPS is used, this intervention becomes impossible due to the encrypted nature of the transmission chain. This encryption renders web browsing more secure and prevents third-party access to data during transmission.

Before the enactment of Law No. 5651, which regulates internet publications in Türkiye, and even after its enforcement, significant difficulties were encountered in the implementation of court orders for access blocking. Court clerks were required to notify each access provider individually, and those providers were expected to enforce the court's decisions. To resolve this chaos and difficulty, Article 90 of Law No. 6518, dated February 6, 2014, amended Law No. 5651 by establishing the "Union of Access Providers." This Union was entrusted with the authority and responsibility to enforce access blocking orders. Furthermore, paragraph 6 of the same law states: "Access blocking orders falling outside the scope of Article 8 of this Law shall be carried out by access providers," thereby explicitly identifying the Union as merely an intermediary institution. The rationale for introducing this additional article is outlined in the Subcommittee report as follows:

"In order to eliminate the problems caused by current practices regarding the removal of content and blocking of access to content — such as unenforceability and uncertainty as to the responsible party — a civil initiative, the Union of Access Providers, is to be established. The goal is to enhance the effectiveness of a civil initiative composed of sector representatives, rather than public

authorities, in implementing precautionary measures concerning internet broadcasts; to ensure alignment with the practices of developed countries; to make it mandatory for all service providers to become members of the Union in order to continue their operations; and to regulate the procedures and principles regarding the established Union.”

As can be seen, the purpose of introducing this article is to ensure the enforcement of court decisions, as is the case in modern states governed by the rule of law and in modern societies. However, the Access Providers Union, which is the body responsible for enforcing access-blocking decisions in Turkey, states that it is unable to block access due to its current infrastructure not permitting the blocking of HTTPS content. Consequently, a decision issued by a Turkish court in accordance with Turkish law cannot be enforced against websites operating in Turkey by a union established under Turkish law and designated as responsible in this area. We believe that one does not need to be a lawyer to recognize the absurdity of this enforcement (or lack thereof).

The Access Providers Union in fact functions as an auxiliary body in terms of the enforcement of court decisions. The primary responsibility for implementing access-blocking decisions lies with content providers. However, as observed in practice, content providers who publish materials violating personal rights often fail to remove such content despite access-blocking decisions issued by the criminal judgeships of peace. The main reasons for this are the unenforceability of the decisions due to the problems posed by the HTTPS protocol and the lack of any sanctions under our legal system against content providers who do not implement court decisions and fail to personally prevent access to the data.

In this context, it is evident that the greatest obstacle to the effective enforcement of legal protections concerning the right to be forgotten lies in the execution of court rulings. What must be done first is to provide the Access Providers Union with the necessary infrastructure to block access to sites using HTTPS. One of the most fundamental requirements of a state governed by the rule of law is the enforcement of court decisions by the highest authorities responsible for applying legal rules. Secondly, Law No. 5651 should include provisions imposing administrative fines and other measures as misdemeanours against content providers who fail to comply with court decisions, and should regulate a criminal offense prescribing custodial sentences and judicial fines for persons responsible for content providers who intentionally disregard such decisions, as well as security measures for legal entities.

C. Regulation Introduced by Article 9/10 of Law No. 5651

With the addition of paragraph 10 to Article 9 of Law No. 5651 by Law No. 7253 dated 29.07.2020, a regulation was introduced that enables individuals to exercise the right to be forgotten with respect to search engines: “In cases where personality rights are violated due to content published on the internet, upon request, the judge may decide that the applicant’s name shall not be associated with the internet addresses that are the subject of the decision under this article.”

Thus, if the violation of personality rights under Article 9 stems from personal data falling within the scope of the right to be forgotten, not only can the content be removed from the online publication, but it may also be removed from search engines displaying that content. The important point to consider when making such a decision is whether the conditions for the right to be forgotten have been met. Accordingly, if concepts such as timeliness or freedom of expression, as explained above, provide a higher benefit than the individual’s right to be forgotten within the scope of a specific application, the content in question should not be removed from search engines even if there is a violation of personality rights.

With the supplementary article added to Law No. 5651 by Law No. 7253 in 2020, regulations were also introduced regarding social network providers. The obligations imposed by this article and the rights granted to individuals, although indirectly, provide new opportunities for the exercise of the right to be forgotten.

CONCLUSION

In the context of the right to the protection of personal data, there were initially debates about the very existence of such a right, whereas the right to be forgotten has now increasingly come to be accepted as a derivative of the right to the protection of personal data. Today, however, new discussions have emerged as to whether the right to be forgotten exists independently as a right in its own standing, separate from the right to data protection.

The right to be forgotten, which has attracted the greatest curiosity and interest among the rights that have emerged with the growing awareness of personal data protection, envisions the erasure of personal data—particularly in the digital sphere. This right represents one of the most recent legal debates raised by information technologies, and it constitutes a new type of right stemming from the capability of digital technologies to ensure that individuals are remembered for a long time through their data.

In the academic literature, it is now argued that the right to be forgotten is distinct from the right to the protection of personal data, yet the two are like two sides of the same coin—separate but inseparably connected rights. We must state that we share this view.

The right to erasure should not be considered the same as the right to be forgotten. Although both rights pertain to personal data and share similarities in terms of the actions to be taken on data upon the exercise of the right, their origins and underlying philosophies are entirely different. It must be noted that this distinction is particularly made by those who oppose the recognition of the right to be forgotten and instead advocate for the right to erasure. According to this view, the right to be forgotten is associated with rewriting history or censorship, whereas the right to erasure concerns more effective and efficient control mechanisms imposed on the state, along with restrictions preventing the excessive commercial retention of data. Therefore, defining this as “forgetting” may be misleading, as erasure pertains not to forgetting, but to control.

As a newly emerging right, the right to be forgotten lacks a universally agreed definition, both in academic literature and international regulations. Moreover, the number of dedicated studies on the subject is particularly limited in Turkey, and the legal regulations that contain this right have yet to reach a level that sufficiently addresses the need. This situation is not only due to the novelty of the right but also to its connection with the field of information law. The dynamic and complex structure of information law makes it a constantly evolving and widely debated domain. In its most general sense, the right to be forgotten is the individual’s request to be forgotten by restricting access to their

personal data. The individual does not wish for certain accessible information about them to be reached or disseminated, for various reasons, and views this as contrary to their interests.

Over time, individuals undergo both physical and psychological changes. Consequently, they may no longer wish to be remembered solely by their “former selves” or, more broadly, by their past. Therefore, the individual’s need to be forgotten, in terms of the passage of time, is not merely a desire but an essential necessity to lead a life free from the burdens of past events. Indeed, Friedrich Nietzsche theorized this need in what he called the “active forgetting thesis.” Nietzsche based the human need to forget on historicity. According to him, the primary difference between humans and animals is the “historicity” factor: Animals lack the concept of historicity and live without sensing a difference between yesterday and today. Humans, on the other hand, possess historical consciousness, and their past is ever-present with them. For Nietzsche, the only condition for achieving happiness is the ability to forget. And human forgetting undoubtedly depends on being forgotten. Only when one is forgotten and no longer remembered for their past can they themselves forget. Therefore, we believe that, with regard to the right to be forgotten, beyond all other elements, the factor of time is crucial in understanding the underlying philosophy and rationale of the right.

Although the right to be forgotten was implicitly included for the first time in Directive 95/46/EC, it essentially came to the fore and began to be debated following the 2014 Google ruling of the Court of Justice of the European Union. Most recently, it was explicitly regulated under the GDPR, which entered into force on 25 May 2018. Thus, for the first time, the right to be forgotten attained legal status as a right under the name “right to erasure.” It should be noted, however, that although the GDPR introduces regulations regarding the erasure of personal data, it does not possess the capacity to resolve the theoretical or philosophical debates concerning the right to be forgotten. Therefore, while the GDPR represents a significant development in terms of providing a legal basis for the right to be forgotten, it must be acknowledged that it cannot, on its own, serve as a comprehensive solution to the issue.

The right to be forgotten, particularly brought to public attention by the 2014 Google ruling of the Court of Justice of the European Union, has since become the subject of numerous national and international regulations and court decisions. With the General Data Protection Regulation, which entered into force on 25 May 2018, the right to be forgotten was granted legal status for the first time under the title “right to erasure.”

In the Google ruling, the Court held that in order to give effect to Articles 12 and 14 of the Directive, the search engine must delete from the displayed list

of results any information published by third parties that pertains to the data subject. Furthermore, in light of Articles 7 and 8 of the Charter of Fundamental Rights, the request to have information concerning the data subject no longer appear in search results is not only related to the search engine's economic interests but also to the public's interest in accessing such information by searching the data subject's name. Therefore, at this point, a balance must be struck between the interference with the data subject's fundamental rights and the overriding interests of the public. To briefly assess the Court's decision, the following findings should be made regarding the right to be forgotten:

For the right to be forgotten to become relevant, there must be a personal data processing activity and a data controller carrying out that activity. Information that was initially published accurately and lawfully may, over time, become a personal data processing activity that is no longer compatible with the Directive. At this point, although the case concerned personal data that was correctly and lawfully disseminated, the judgment does not clarify whether the right to be forgotten would also apply to data that had been published incorrectly or unlawfully. Personal data that becomes incompatible with the Directive typically includes data that is no longer necessary for the purposes for which it was collected or processed, data that becomes inadequate, irrelevant, or excessive in relation to those purposes in light of the time that has passed. In such a case, it must be acknowledged that the data subject has a right to request that the information no longer be made available to the public. The Court established the legal basis of the right to be forgotten by stating that this right arises from a joint assessment of Articles 12 and 14 of the Directive along with Articles 7 and 8 of the Charter of Fundamental Rights. Finally, a balance must be struck between the data subject's request not to have their information made public and the economic interests of the search engine operator, as well as the public's interest in accessing such information. In this way, by revealing the relationship of the right to be forgotten with other rights and freedoms, the Court laid the foundation for the exceptions to the right, as will be discussed below. On the other hand, it becomes clear that the right is not absolute.

There are numerous rulings of the ECtHR and the CJEU regarding the right to be forgotten. In addition, in Türkiye, both the Constitutional Court and the Court of Cassation's General Assembly of Civil Chambers have delivered decisions concerning this right. Although the Personal Data Protection Law does not explicitly address the right to be forgotten, the courts have attempted to define its scope and content through case law. The Personal Data Protection Board has also indirectly regulated this right through the issuance of the "Regulation on the Deletion, Destruction and Anonymization of Personal Data."

An important development in both doctrine and practice regarding this issue is the emerging tendency to avoid excessive application of the right to be forgotten. This tendency is particularly evident in the ECtHR's judgment of 28 July 2018 in the case of *M.L. and W.W. v. Germany*. In response to the applicants' claim that their right to be forgotten had been violated due to a crime they committed in the past, the Court found that there was a prevailing public interest. At the time, public attention to the event was considerable, and the fact that the content was published up until shortly before the applicants' release indicated that the public was interested not only in current events but also in researching past incidents. Within this context, the press has the duty to contribute to democratic discourse by granting access to publicly available archived news content. Public access to such archived news is a consequence of the freedom of expression guaranteed by Article 10 of the ECHR. As a result, the Court held that the applicants' rights had not been violated due to these and related reasons. Therefore, this right is not unlimited, and not every request related to the right to be forgotten can be fulfilled—neither technically nor in light of the public's overriding interest in the matter. This is a well-founded judgment and perspective for defining the scope of the right to be forgotten, which may at first appear to be absolute.

There are opinions asserting that the right to be forgotten does not actually entail the removal or destruction of the personal data in question, but rather the delisting of such data from search results in response to specific queries. According to this view, the EU's so-called "right to be forgotten" merely requires the deletion of information from search engines and does not mandate full removal by the content provider.

As a result, the relevant websites technically remain accessible but are no longer indexed in search results. This is seen as a relative balance between the interests of freedom of speech and privacy. Indeed, this is also the case in the CJEU's Google ruling. Google interpreted the judgment as requiring that, when a data subject exercises the right to be forgotten, the personal data in question should not appear in search results conducted using the subject's name. Thus, the data that is meant to be forgotten still exists and remains accessible, but it is not displayed to users conducting certain types of searches. This approach has been criticized on the grounds that it does not enable true forgetting. Indeed, if information is simply omitted from search results conducted using, for example, the data subject's name—but remains accessible through other types of queries—it is difficult to speak of true erasure. While this may have some effect in limiting dissemination and accessibility, if the data can still be accessed through alternative searches, it is very difficult for the right to be forgotten to truly achieve its intended purpose. Nevertheless, the freedom of the internet and

the need to balance this right with other conflicting rights and freedoms necessitate such a limitation.

In concluding this study, the most significant insight we have reached is that we are still at the very beginning of this journey and much remains to be said on the matter.

BIBLIOGRAPHY

BOOKS AND ARTICLES

- Alessi**, Stefania, “Eternal Sunshine: The Right to be Forgotten in the European Union after the 2016 General Data Protection Regulation”, *Emory International Law Review*, V. 32, 2017.
- Alsenoy**, Brendan van, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, Cambridge – Antwerp – Chicago, 2019.
- Arslan**, Kahan Onur, “İnsan Onuru ve Koruma Tedbirleri Bağlamında Temel Bir İlke Olarak İnsan Onurunun Korunması”, *Türkiye Barolar Birliği Dergisi*, S. 120, 2015.
- Ausloos**, Jef, *The Right to Erasure in EU Data Protection Law*, Oxford University Press, Oxford, 2020.
- Barnes**, Susan B., *A Privacy Paradox: Social Networking in the United States*, 2006, https://firstmonday.org/article/view/1394/1312_2.
- Bernal**, Paul, *Internet Privacy Rights - Rights to Protect Autonomy*, Cambridge University Press, Cambridge, 2014.
- Bozkurt Yüksel**, Armağan Ebru, *Bulut Bilişimde Kişisel Verilerin Korunması*, Yetkin, Ankara, 2016.
- Carter**, Edward L., “The Right To Be Forgotten”, <http://oxfordre.com/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-189>; 09.03.2019.
- Değirmenci**, Olgun, *Yargısal İçtihatların Ortaya Çıkardığı Bir Hak: Unutulma Hakkı (Çerçevesi ve Hak Üzerine Düşünceler)*, *Terazi Hukuk Dergisi*, C.13, S. 144, Ağustos, 2018, 153-163.
- De Terwangne**, Cécile, “The Right to be Forgotten and Informational Autonomy in the Digital Environment”, *The Ethics of Memory in a Digital Age Interrogating the Right to be Forgotten*, Ed. AlessiaGhezzi/ÂngelaGuimarãesPereira/Lucia Vesnić-Alujević, European Commission, Joint Research Centre, Palgrave Macmillan, New York, 2014.
- De Terwangne**, Cécile/Jean-Philippe Moyny, *Report on the Consultation on the Modernisation of Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Council of Europe, Strasbourg, 2011.
- Donnelly**, Jack, *Universal Human Rights In Theory and Practice*, 3. Ed., Cornell University Press, Ithaca and London, 2013.
- Dutertre**, Gilles, *Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler*, Avrupa Konseyi Yayınları, 2013.

- Dölger**, Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019.
- Dölger**, Murat Volkan, “İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması”, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Y. 5, S. 1, Bahar 2018.
- Eltis**, Karen/Pierre Trudel, Canadian Report: Delisting in the Digital Age – A Hybrid Approach to Bridge the European and American Visions of the “Right to be Forgotten”, International Academy of Comparative Law - Fukuoka Congress, 2018.
- Etzioni**, Amitai, Privacy in a Cyber Age, Palgrave Macmillan, New York, 2015.
- Fleischer**, Peter, “The Right to be Forgotten, or How to Edit Your History” <http://peterfleischer.blogspot.com/2012/01/right-to-be-forgotten-or-how-to-edit.html>, 10.03.2019.
- Gajda**, Amy, “Privacy, Press, and the Right to Be Forgotten in the United States”, Washington Law Review, Vol. 93, 2018, 201-264.
- Gümüş**, Ali Tarık, “Türk Anayasasında Kişinin Maddi ve Manevi Varlığını Koruma Geliştirme Hakkı”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 13, S. 2, 2005.
- Hartzog**, Woodrow, Privacy’s Blueprint: The Battle to Control the Design of New Technologies, Harvard University Press, Cambridge, 2018.
- Herlocker**, Jack: “Stacy Snyder and the Untruth That Won't Die”, September 22, 2015, <https://medium.com/@jherlocker/stacy-snyder-and-the-untruth-that-won-t-die-549c2f525661>.
- Hornung**, Gerrit/Christoph Schnabel, “Data Protection in Germany I: The Population Census Decision and the Right to Informational Self Determination”, Computer Law & Security Review, Vol. 25, 2009.
- Hugo**, Victor, Sefiller, Çev. Volkan Yalçıntoklu, 8. Baskı, Türkiye İş Bankası Yayınları, İstanbul, 2019.
- Jones**, Meg Leta, Ctrl + Z: The Right to Be Forgotten, New York University Press, New York, 2016.
- Lloyd-Jones**, Heledd/Peter Carey, “The Rights of Individuals”, Data Protection: A Practical Guide to UK Law, Ed: Peter Carey, 5. Baskı, Oxford University Press, Oxford, 2018.
- Lynskey**, Orla, The Foundations of EU Data Protection Law, Oxford University Press, Oxford, 2015.
- Martin**, Yod-Samuel/Jose M. del Alamo, “Forget About Being Forgetting: From the Right to Oblivion to the Right of Reply”, Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection, Ed: Serge Gutwirth / Ronald Leenes / Paul De Hert, Springer, Heidelberg, 2016.
- Mayer-Schönberger**, Viktor, Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, New Jersey, 2009.

- Mkadmi**, Abderrazak, Preservation and the Right to be Forgotten, Archives in The Digital Age, Volume 8, John Wiley & Sons, London, 2021.
- Nietzsche**, Friedrich, Hayat Dediğın Nedir Ki?, Çev. Erkan Aslan, Aylak Adam, İstanbul, 2015.
- Nietzsche**, Friedrich, On the Advantage and Disadvantage of History for Life, Translated by. Peter Preuss, 15. Baskı, Hackett Pub Co, Cambridge, 1980.
- Quinn**, Sarah, “Facebook costing 16-34s jobs in tougheconomicclimate”, <https://ondeviceresearch.com/blog/facebook-costing-16-34s-jobs-in-tough-economic-climate>, 10.03.2019.
- Pagallo**, Ugo, “The Impact of Domestic Robots on Privacy and Data Protection, and the Troubles with Legal Regulationby Design”, Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection, Ed. Serge Gutwirth/Ronald Leenes/Paul De Hert, Springer, Heidelberg, 2016.
- Pereira**, Ângela Guimarães/Lucia Vesnić-Alujevića/Alessia Ghezzi, “The Ethics of Forgetting and Remembering in the Digital World through the Eye of the Media”, The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten, Ed. Alessia Ghezzi/Ângela Guimarães Pereira/Lucia Vesnić-Alujević, Palgrave Macmillan, Hampshire, 2014.
- Post**, Robert C., “Data Privacy and Dignitary Privacy: Google Spain, The Right to be Forgotten, and the Construction of the Public Sphere”, Duke Law Journal, V. 67, 2018, 981-1072.
- Roagna**, Ivana, Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması, Avrupa Konseyi İnsan Hakları El Kitapları, Strazburg, Avrupa Konseyi Yayını, 2012.
- Sloot**, Bart van der, “Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR’s Case Law on Privacy Violations Arising from Surveillance Activities”, Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection, Ed. Serge Gutwirth / Ronald Leenes / Paul De Hert, Springer, Heidelberg, 2016.
- Sözüier**, Eren, Unutulma Hakkı: İnsan Hakları Hukuku Perspektifinden Bir İnceleme, On İki Levha Yayıncılık, Ankara, 2017.
- Taylor**, Roger, “No Privacy without Transparency”, Data Protectionand Privacy: The Age of Intelligent Machines, Ed. Ronald Leenes/Rosamunde van Brakel/Serge Gutwirth/Paul De Hert, Hart Publishing, Oxford, 2017.
- Tene**, Omer, “What Google Knows: Privacy and Internet Search Engines”, Utah Law Review, No. 4, 2008, 1433-1493,
- Travis**, Alan/Charles Arthur, “EU Court Backs ‘Right to Be Forgotten’: Google Must Amend Results on Request, 2014, <https://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results>.
- Turgut**, Cemile, Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı, On İki Levha Yayıncılık, İstanbul, 2021.
- Voigt**, Paul/Axel von dem Bussche, The EU General Data Protection Regulation (GDPR), Springer, 2017.

- Weber**, Rolf H., The Right to be Forgotten: More Than a Pandora's Box?, 2011.
- Werro**, Franz, "The Right to Be Forgotten: The General Report—Congress of the International Society of Comparative Law", in: The Right To Be Forgotten A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia, Ed. Franz Werro, Springer, Charm, 2020, 1-35.
- Whitman**, James Q., "The Two Western Cultures of Privacy: Dignity versus Liberty", Yale Law Journal, Vol. 113, No. 6, 2004, 1151-1221.
- Yavuz**, Can, İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması: Unutulma Hakkı, Seçkin Yayıncılık, Ankara, 2016.