Palacký University in Olomouc
Faculty of Law

Hovsep Kocharyan

The Development of the Right to be Forgotten in EU law: Challenges and Perspectives

Doctoral Dissertation

Olomouc 2023

Declaration of Originality

I declare that the dissertation is my original work entitled by “The Development of the Right to be Forgotten in the EU Law: Challenges and Perspectives ”. The literature resources used in this work are clearly quoted in both the text and references.

In Olomouc 29. 12. 2023 Hovsep Kocharyan

I would like to thank to my supervisor JUDr. Ondrej Hamuľák, Ph.D. for his tangible guidance throughout this thesis. The greatest thanks are given to my family for their unreserved encouragement.

Table of Contents

1 Introduction

Since the advent of the Internet, the issue of human privacy in legal science remains one of the most controversial and problematic. The processing of personal data on the Internet is becoming more common, and nowadays it is an inevitable part of human life. Proper protection of human personal data within EU especially on the Internet, requires solving the problem of constant disclosure of such data. As soon as personal data is disclosed (primarily in the field of the Internet), it is usually available for an indefinite period of time. However, this practice creates serious risks of violating the right to privacy of a person. The right to be forgotten, particularly in relation to digital space and internet activities, is a new legal phenomenon that reaches high relevance within the contemporary legal research.

Nowadays, more than ever, a comprehensive and detailed analysis of this right in the current legal reality of the EU is more than necessary. This need is due to the fact that the question of the correlation of the right to be forgotten (as the new "internet" human right) with such classical human rights as respect for private and family life, protection of personal data, freedom of expression and information is brought to the fore.[1]

On the one hand, Article 11 of the CFR enshrines freedom of expression and information, but on the other hand, the case law of the CJEU recognizes the existence of the right to be forgotten. The question naturally arises: How does the right to be forgotten relate to the above-mentioned fundamental human rights? Do the criteria for the application of the right to be forgotten set out in the EU legislation [2] and the case law[3] of the CJEU allow to minimize the risk of conflicts between these rights?

Besides, recently considering the cases of *Google LLC v CNIL*[4] and *Glawischnig-Piesczek v Facebook*[5] the CJEU stated its position concerning the territorial scope of application of the right to be forgotten in the following way. So, in the case of *Google LLC v CNIL* the CJEU held that the right to be forgotten under the DPD and the GDPR does not require a search engine provider to carry out global de-referencing but only in respect of those versions of its

[1] See Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union (2012/C 326/02) (CFR). [online]. Accessible at: <http://data.europa.eu/eli/treaty/char_2012/oj>
[2] Primarily in Article 17 of the General Data Protection Regulation ((EU) 2016/679
[3] Primarily in the cases C 131/12; C-507/17 and C-18/18)
[4] Court of Justice of the European Union: Judgment of 24th September 2019. *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*. Case C-507/17.
[5] Court of Justice of the European Union: Judgment of 3th October 2019. *Eva Glawischnig-Piesczek v Facebook Ireland Limited.* Case C-18/18.

search engine that correspond to EU Member States,[6] thereby limiting the right to be forgotten to the territory of the EU. However, nine days later (on 3th October 2019), in the *Glawischnig-Piesczek v Facebook* case the CJEU ruled that in the context of take-down of online defamatory content, EU Member States can decide themselves whether it is appropriate to give worldwide effect to injunctions stipulating the take down of illegal defamatory content from host provider platforms.[7]

Analysing the positions of the CJEU on the abovementioned cases, some researchers see a certain confusion and even contradiction regarding the territorial scope of application of the right to be forgotten,[8] while others deny the existence of such inconsistencies in the judicial practice of the Court.[9] In this situation there is another question: is there any inconsistency or contradiction in the positions of the CJEU regarding the territorial scope of application of the right to be forgotten, and if so, how such inconsistency or contradiction can be resolved? In this regard, I conduct a comprehensive analysis of the current EU legislation and, first of all, the case law of the CJEU on the right to be forgotten. This thesis clearly identifies the essence and nature of the right to be forgotten, its essence, the problematic aspects of the correlation between the right to be forgotten and the right to respect for private and family life, freedom of expression and information, as well as the problems of territorial scope of the right to be forgotten and will offer solutions.

Finally, it should be noted that the judicial approaches of both the CJEU and the ECtHR play a fundamental role in the process of forming of the European standards for the protection of human rights. Although the case law of both European Supranational Courts is constantly evolving, and the Courts are not able to keep up with the progress of digital technologies. This means that the judicial approaches developed by the Courts for the offline world should somehow be adopted for the online world as well, in order to avoid the risks of violating fundamental human rights such as respect for private and family life, protection of personal

---

[6] Court of Justice of the European Union: Judgment of 24th September 2019. *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*. Case C-507/17, para. 73

[7] Court of Justice of the European Union: Judgment of 3th October 2019. *Eva Glawischnig-Piesczek v Facebook Ireland Limited.* Case C-18/18., para. 46 and 53.

[8] JUSTIN, Clark et al. *Content and Conduct: How English Wikipedia Moderates Harmful Speech*. Harvard University, Berkman Klein Center for Internet & Society, 2019, 76 p.; KETTEMANN, Matthias C.; Tiedeke, SOPHIA Anna. *Welche Regeln, welches Recht? Glawischnig-Piesczek und die Gefahren nationaler Jurisdiktionskonflikte im Internet* [online]. VerfBlog, 10th October 2019 [cit. on. 16th December 2023]. Accessible at: <https://verfassungsblog.de/welche-rechte-welches-recht/>.

[9] HOPKINS, Cathryn. *Territorial scope in recent CJEU cases: Google v CNIL / Glawischnig-Piesczek v Facebook* [online]. The International Forum for Responsible Media Blog, 9th November 2019 [cit. on. 16th December 2023]. Accessible at: <https://inforrm.org/2019/11/09/territorial-scope-in-recent-cjeu-cases-google-v-cnil-glawischnig-piesczek-v-facebook-cathryn-hopkins/>.

data and freedom of expression and freedom of information in the future. Taking into account the above, I consider it necessary to conduct a comparative and in-depth analysis of the judicial approaches of both European Supranational Courts regarding the phenomenon of the right to be forgotten in order to determine its place in the human rights system, to point out problematic aspects of its correlation with other human rights and new prospects for its development, as well as to propose reasoned ways of their solution.

1.1 Research goal and questions

A large number of scientific researches are devoted to the analysing of the essence and nature of the right to be forgotten, as well as the issues of its legal protection in Europe.[10] The scientific interest on this topic has increased after the entry into force of the GDPR and the latest development of the judicial practice of the CJEU regarding the right to be forgotten.[11] Some researchers are aimed to explore the issues of the territorial scope of application of this right.[12] Although it should be noted that because of different approaches of the researchers on the essence and nature of the right to be forgotten as well as to the issues of its territorial application,[13] this topic still remains relevant and debatable in the legal doctrine.

The originality of this thesis lies in the fact that I undertake a comprehensive and detailed analysis of the phenomenon of right to be forgotten with in-depth analysis of judicial

---

[10] IGLEZAKIS, Ioannis. *The Right to be Forgotten: A New Digital Right for Cyberspace* [online]. Segurança da informação e Direito Constitucional do ciberespaço, 26th December 2016 [cit. on 16th December 2023]// Accessible at: <https://iglezakis.gr/2016/12/26/the-right-to-be-forgotten-a-new-digital-right-for-cyberspace/>; WECHSLER, Simon. The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten. Columbia Journal of Law and Social Problems, 2015, Vol. 49, pp. 135-165; DE TERWANGNE, Cécile. The right to be forgotten and the Informational Autonomy in the Digital Environment. Publication office of the EU, 2013, Vol. 13, pp. 1-30.

[11] PADOVA, Yann. Is the right to be forgotten a universal, regional, or 'glocal' right?, International Data Privacy Law, 2019, Vol. 0, No. 0, pp. 1-15; TAYLOR, Mistale. Reasonableness in its reasoning: How the European Union can mitigate problematic extraterritoriality on a de-territorialised internet. Questions of International Law, 2019, Vol. 62, pp. 35-53.

[12] TAYLOR, Mistale. Reasonableness in its reasoning: How the European Union can mitigate problematic extraterritoriality on a de-territorialised internet. Questions of International Law, 2019, vol. 62, pp. 35-53.; SAMONTE, Mary. *Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law* [online]. European Law Blog, 29th October 2019 [cit. on 16th December 2023]// Accessible at: <https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/>.

[13] KETTEMANN, Matthias C.; Tiedeke, SOPHIA Anna. *Welche Regeln, welches Recht? Glawischnig-Piesczek und die Gefahren nationaler Jurisdiktionskonflikte im Internet* [online]. VerfBlog, 10th October 2019 [cit. on. 16th December 2023]. Accessible at: <https://verfassungsblog.de/welche-rechte-welches-recht/>; HOPKINS, Cathryn. *Territorial scope in recent CJEU cases: Google v CNIL / Glawischnig-Piesczek v Facebook* [online]. The International Forum for Responsible Media Blog, 9th November 2019 [cit. on. 16th December 2023]. Accessible at: <https://inforrm.org/2019/11/09/territorial-scope-in-recent-cjeu-cases-google-v-cnil-glawischnig-piesczek-v-facebook-cathryn-hopkins/>.

approaches of not only the CJEU, but also the ECtHR, in order to clearly show the problematic aspects and new challenges of legal protection of the right to be forgotten in Europe and suggest ways to resolve them. In this regard the research will attempt to clarify the following issues:

1. the material scope of the right to be forgotten, its essence, justifications, definitions and problematic aspects of its regulation before and after GDPR;
2. the territorial scope (global aspirations) of the application of the right to be forgotten and its balancing with freedom of expression taking into account the judicial practice of both the CJEU and the ECtHR;
3. in-depth comparison of the judicial approaches of the key judicial players (namely the CJEU and the ECtHR) regarding the phenomenon of the right to be forgotten.

The goal of the thesis is to identify:

1. the essence and nature of the right to be forgotten, its scope, justification, its place in the system of protection of human rights;
2. the issues of effective judicial protection of the right to be forgotten in the current EU legislation, and, first and foremost, in the judicial practice of the CJEU;
3. the problematic aspects of its correlation between the right to be forgotten with the right to respect for private and family life, freedom of expression and information; analysis of problematic aspects of territorial scope of application taking to account the latest judicial practice of the CJEU and ECtHR;
4. new challenges in development of the right and suggest ways for their solution.

Particular attention is paid to the comparison of judicial approaches of the CJEU and the ECHR to the phenomenon of the right to be forgotten. To achieve the above goals of the research, the following tasks were set:

1. analysis of the evolution of the right to be forgotten before and after the entry into force of the GDPR, its interpretation and application in the judicial practice of the CJEU;
2. analysis of problematic aspects of legal regulation of the right to be forgotten within the EU before and after the entry into force of the GDPR with mandatory consideration of the existing judicial practice of the CJEU and ECtHR;
3. preparation of recommendations to solve the problems identified in the research, as well as a reasoned indication of the ways to further develop of the protection of the right to be forgotten within the EU;

4. preparation of recommendations for improving the effectiveness in the field of protection of the right to be forgotten.

In this study, I attempt to answer the following questions:

1. What is the right to be forgotten?
2. What are the problematic aspects of the correlation between the right to be forgotten and respect for private and family life and freedom of expression and information within the EU, and how they can be solved?
3. What are the risks of effective judicial protection of the right to be forgotten created by the contemporary case law of the CJEU and ECtHR, and how they can be solved?

1.2 Thesis hypotheses

Within the thesis I use several approaches to meet the complex issues of the thesis focus. As a starting point (especially when working with the set of relevant data/documents) I utilise the analytical approach (the desktop research) in order to identify, systematise and mutually compare the key case-law, its impact and interpretations.

Hypotheses of the thesis are:

1. The Right to be forgotten has a potential to serve as legal mechanism, allowing the deletion of personal data left on the Internet in order to protect the individual, his dignity, reputation, privacy and identity in the online world.
2. There are visible distinctions in understanding of the scope and content of the Right to be forgotten in the relevant case law of key European supranational courts.

Both hypotheses are tested in parallel via critical analyses of the case-law and its developments.

1.3 Methodology of the thesis

For a more complete disclosure of the content of the thesis topic, historical, comparative, normative, logical methods, as well as the method of system-structural analysis are used. In the thesis, the doctrine of positivistic analysis in law is used as a scientific tool. From this point of view, a special value is the normative approach to the analysis of the subject of research, the

development of scientific and legal concepts, the construction of conclusions based on legal reasoning. The comparative method is fundamental in the analysis of individual judgments of the CJEU and the ECtHR.

During all phases of the thesis, I employ the traditional processes of the evolution of the thesis outcomes, i.e.:

- deductive approach while testing the hypotheses against the assembled data;
- inductive methods while formulating the models of interpretation;
- comparative methods, while comparing the approach of key stakeholders;
- synthesis, while working on the conclusions and defining the nature, contours and scope of the right to be forgotten;
- prediction in evaluation and extrapolation of the future challenges and developments.

1.4 Theoretical and practical significance of the thesis

The thesis makes a certain contribution to the science of the EU law through the study and synthesis of new theoretical and empirical material on the basis of systematisation of the current EU legislation and judicial practice of the CJEU. The theoretical significance of the thesis contributes to the development and deepening of modern theoretical ideas about the right to be forgotten, the problems of correlation with fundamental human rights within the EU. On the basis of a comparative analysis of the case-law of the CJEU and the ECtHR, the main risks and vectors of the development of the right to be forgotten in the EU law will be identified.

The thesis also contributes to the development of the theoretical study of the CFR provisions, deepening the theoretical foundations of the EU human rights law in the field of Internet. In particular, the analysis of the human rights catalogues enshrined in the CFR will reveal problematic aspects of the correlation between the right to be forgotten and such fundamental human rights as respect for private and family life, protection of personal data, freedom of expression and information. These rights will identify the risks of effective protection of the right to be forgotten as a result of the analysis of the case law of the CJEU and the ECtHR will offer theoretically justified proposed solutions.

Timely identification and analysis of the remaining unsolved problems and development of recommendations for their possible solution can be used by the relevant institutions in developing positions and improving the normative regulation of legal relations

in the designated area. The findings of the study may further contribute to more effective protection of human rights in the Internet environment within the EU.

The obtained results will complement and develop existing concepts of human rights protection mechanisms not only in the science of the EU law, but also in other legal disciplines, and can be used in the preparation of materials for lectures and seminars for students studying human rights and the EU law.

1.5 Description of the structure and content of the thesis

The thesis consists of an introduction, five chapters and a conclusion. The text of the thesis is additionally supplemented with a list of references, a list of keywords and an abstract.

The general introduction, including the statement of research objectives, definition of research problems, hypothesis and description of the thesis content, is followed by the Chapter *"Privacy in the digital society: concepts and new foundations"*, which presents a brief course of the development of the right to privacy, classifies the features of the main privacy concepts, identifies the main risks to privacy and data protection in the context of the datafication of society.

The concept of privacy is related to the level of technology development and its use in everyday life. In total, privacy is a dynamic concept with a tendency to constant transformation. The reconfiguration of the elements underlying the understanding of privacy has been ongoing, and new combinations of technologies, meanings, and practices have led to a shift in boundaries between what is considered public or private space. Nowadays data protection has become one of the main approaches to regulating the protection of privacy and confidentiality in EU law.

Next, I consider the basic doctrinal concepts of privacy. Being an almost indefinite legal category, privacy makes it possible to be widely used in various situations, including those arising from the rapid development and introduction of technologies, while not limiting the application of the law or weakening human protection. This uncertainty has led to a situation where various concepts of privacy have appeared in the doctrine of law, which can be grouped into ontological categories. I come to the conclusion that if traditionally the interests of privacy were implied in the legal or social protection of personal property and space, intimate surroundings or personal effects, then modern concepts of privacy are closely related to technological developments that allow for a new invasion of intimate aspects of life.

Looking at some of the concepts, I come to the conclusion that special attention should also be paid to the concept of social privacy, where privacy is the right of individuals, groups or organizations to make discretionary decisions about when, how and to what extent their personal information will be disclosed to others. This concept has the advantage that the discussion about the right to be forgotten also covers aspects relevant to groups and organizations, especially with the widespread use of Big Data analytics technology.

Next, I consider some of the risks that appear in modern society in the process of digitalisation. Among the privacy risks resulting from datafication, the separation of regulation of data transmission processes in the public and private sectors is becoming increasingly difficult. The spread of data is blurring the boundaries between citizens and consumers, as more and more government services begin to rely on platforms provided by corporations. This indicates the connection between privacy and power. Another consequence of the impact of datafication on everyday life is the transformation of privacy and data into a commodity that can be sold.

Content on the Internet does not have a natural expiration of time and people face their past for a long time, because they cannot completely change their digital footprint. Such long-term information can indicate a person's interpersonal relationships and his/her social status. Among the mechanisms for levelling the above-mentioned risks to the person in the context of datafication and extensive information collection, a special place is occupied by the right to be forgotten, which becomes one of the main mechanisms for preventing potential damage to human rights and his personality in the context of the datafication of society.

The Chapter *"Introducing the right to be forgotten"* begins with an exploration of the essence and justification of the right to be forgotten. I point out that from the very beginning, the right to be forgotten was justified by privacy, which can be seen in the judicial practice of the ECtHR. In EU law, especially after the adoption of the EU Charter, the right to be forgotten receives a new justification, becoming a specification of the right to personal data protection. Recognising the protection of personal data as a fundamental right goes beyond the general protection of privacy. First of all, "economic logic" led to the constitutionalising of data protection. Nevertheless, the recognition of fundamentality did not solve the issue of individual protection and did not reach the logic that led to its fundamentality. Although the right to be forgotten, as a concretisation of the fundamental right to data protection, should primarily regulate the relationship between the individual and the state, the GDPR makes it, in particular, one of the mechanisms for regulating the relationship between the private interests of the data controller (data processor) and the data subject himself/herself. Moreover, the legal regulation

proposed by the GDPR puts these private entities in an unequal position from the very beginning. In addition, the right to be forgotten in EU law, despite the fact that it is a specification of the fundamental right to data protection, nevertheless it is also an instrument of market regulation and redistribution of powers between data subjects and data processors, and has the prerequisites for becoming a collective right.

Some elements of the right to be forgotten can be traced in the concept of the right to information self-determination, however, it is impossible to exercise full control due to important limitations of the rights themselves provided for in the GDPR. Thus, the right to be forgotten can be exercised in one of a limited number of situations. Therefore, it is not possible to say that data subjects have a general right to request the deletion of their personal data or object to the processing of their personal data.

I come to the conclusion that the justification for the right to be forgotten can be the concept of the right to personal identity. In this context, the right to be forgotten can expand its scope and gain a new dimension of essence. The recognition of a person's digital identity as a justification for the right to be forgotten corresponds to the case law of the CJEU, which views the right to be forgotten as a certain emphasis on the assumption of the possibility of "managing" a digital person.

Based on the above, I conclude that the originally conceived right to be forgotten as the right to "forget one's criminal past" has, with the development of the Internet, gained the potential to become a broader right with greater possibilities and potential, acquiring a different essence as a response to the contemporary challenges of the "non-forgetting" Internet.

Next, the theoretical definitions of the right to be forgotten are considered. It is indicated that there is no unambiguous definition. From a theoretical point of view, the definition of the right to be forgotten primarily encounters terminological diversity, which is used both in doctrine and in normative acts.

There are two leading schools of thought that consider the different ontological scope of the right to be forgotten. The first considers it as an extension of the right to delete, while the second considers it as an annoying misunderstanding, the supporters of which insist that the *Google Spain* case simply clarified the scope of the right to delete, while not taking into account the case law of the ECtHR. The simultaneous use of such a multitude of terms that are not only undefined, but also sometimes carry different semantic meanings make the law in question uncertain.

Critically considering the main points of the *Google Spain* case, it seems to me that the significance of this judgment in determining the right to be forgotten is somewhat exaggerated,

because it was issued under the procedure of Article 267 of the TFEU and did not create a precedent in accordance with the "*stare decisis*".

The CJEU has practically delimited the definition of the contours of the right to be forgotten by search engines. Thus, private organizations have become a kind of legislator for the right to be forgotten. The CJEU also failed to clarify the cases and circumstances in which the prevailing public interest would require constant access to information and when instead the information is no longer relevant. The uncertainties in interpretation were not eliminated in Article 17 of the GDPR.

In the absence of any legally established right to be forgotten and criteria for balancing it with other rights, the Court began to form the scope of this right through its law enforcement practice.

The subsequent practice of the CJEU confirms the right to be forgotten in the EU legal order, expanding the scope of its application. Although the decisions of the CJEU can be seen as a logical and consistent step in expanding the case law of the CJEU on this issue after the *Google Spain* case, nevertheless, the right to be forgotten in the EU and beyond also highlights the lack of a common vision of the right in question. The lack of a suitable regulatory framework for defining its contours cannot be considered correct.

The Chapter *"The scope of application of the right to be forgotten in practice"* examines the scope of the right to be forgotten, as well as reveals the concept of personal data and its elements. It is concluded that the CJEU adheres to a broad interpretation of the elements of the definition of personal data, which makes it possible to extend the right to be forgotten to a broader area of personal data protection than indicated in case-law of the CJEU.

In the Chapter *"Finding a balance between the right to be forgotten and freedom of expression"* I focus on examining aspects of finding the necessary balance of rights between the right to be forgotten and the right to freedom of expression, starting with the *Google Spain* case. The wording given by the CJEU in the *Google Spain* case did not resolve the issues of contradiction between the rights in question. Firstly, the prevailing interest of the general public in access to information is not due solely to the role of the data subject in public life. This is only one of the possible reasons, but there may be other "special reasons" similar in importance or substance to the role indicated by the CJEU. The permissibility of possible situations does not make it possible to unambiguously decide how much weight one right should have in relation to another. Secondly, the CJEU has not developed any criterion for determining the priority between the "public interest" and the "right to be forgotten" when public and private interests compete, especially when there is no direct separation between public and private

interests. Thirdly, the CJEU only mentioned the principle of a public figure, according to which the applicant's social position or public activities of the applicant may generate public interest, which may outweigh the right to be forgotten. Fourthly, in determining the right to be forgotten, the CJEU distinguished the right only within the framework of search, which is carried out through search engines, and not in a broader sense. This means that data deletion is only possible in relation to search engine listings, while the information itself may remain on the Internet.

Having analysed the practice of the CJEU and the ECtHR, I come to the conclusion that the grounds referred to by the CJEU in its practice, especially after the judgment in the *Google Spain* case, differ from the grounds referred to by the ECtHR when considering the right to be forgotten. The theoretical basis of the ECtHR's argument focuses on ensuring a balance between the right to public discussion and the damage caused by publication, and applying the standard of serious damage to assess damage. In particular, the damage caused must reach a certain level in order to become a significant factor regarding the violation of the right to privacy. In addition, the ECtHR considers the position of search engines only in passing, limiting itself to the statement that due to their reinforcing effect on the dissemination of information, the obligations of search engines to a person claiming the right to be forgotten may differ from the obligations of the original publisher of information.

In the Chapter *"The right to be forgotten: challenges and prospects for EU Data protection law"*, the right to be forgotten is primarily considered as a mechanism to ensure personal identity. The development of information technology has led to the emergence of the "digital person". With the help of these technologies, a person's identity is "assembled" from his/her "digital parts". The advent of the Internet of Things ("IoT") and the Internet of the Body ("IoB") are changing and expanding the ways and tools of expressing, representing and projecting a person's identity from third parties, especially for marketing.

Moreover, the creation of a digital profile of a person is practically independent of his/her actions or consent. Getting out of control and the sphere of human control, the elements of his/her identity become an object of appropriation, falsification, making a person more vulnerable.

At the same time, the same information technologies have given the person himself/herself the opportunity to project his/her identity in the digital space, for example, also through the right to be forgotten. Such a projection involves the creation of self-images in the digital space that reveal the elements of a person's personality. With the creation of these self-images, a person's digital life enters into another aspect of human existence, which, although

closely related to traditional life, is nevertheless characterized by specific interactions with other people. The personal data that make up a person's digital life are not just data – they are the constituent elements of a digital personality.

The life of a modern person gets another dimension – a digital one. It is impossible to legally protect one dimension and ignore the other. Creating or choosing one's own content for one's digital identity involves providing a person with the legal tools with which he/she creates and protects his/her choice. The informational nature of identity makes it a matter of data processing and information management, therefore, many legal mechanisms that are provided and applied in the context of personal data protection can become legal tools for protecting identity, including the right to be forgotten. For such a fundamental protection of the individual, it is proposed that the protection should be justified.

In its case law, the CJEU reflects on the right to be forgotten as a certain emphasis on the assumption of the possibility of "managing" a digital person, and the right to be forgotten becomes one of the tools for the formation of digital identity. Considering the right to be forgotten in this way can expand the scope of its application, become a so-called paradigmatic shift from the justification of privacy and confidentiality to the justification of identity. First of all, this concerns improving efficiency in balancing the right to be forgotten with the right to express opinions and access to information.

Considering the issues of *post-mortem* privacy, it is indicated that people leave digital traces even after their death and the preservation of this information contributes to the survival of the digital identity of the deceased. The biological body may no longer exist, but feelings, consciousness, actions and will exist and will constantly exist in the digital world as expressions of human identity.

However, within the existing legal framework, protecting this aspect will be a very difficult task. The GDPR has left the issue of posthumous protection of personal data without due attention, leaving the issue of posthumous protection of personal data at the discretion of the EU member States. The inconsistency of judicial practice in this matter also makes it impossible to unambiguously conclude that the right to be forgotten is allowed for the deceased person.

Nevertheless, the approach of the EU legislator is theoretically connected with the assumption that the deceased cannot have or exercise personal rights. However, this approach is already being questioned today. It seems to me that the approach that is generally accepted in EU law is no longer correct in the light of the development of a networked society and the phenomenological gap between online and offline human presence justifies efforts to solve

problems of legal qualification of tools and remedies that can be applied to ensure effective posthumous protection of human rights in the digital sphere, including the right to be forgotten. In considering the issue of *post-mortem* data protection in the legal doctrine, I point out that one of the arguments that opponents of the right to *post-mortem* privacy point to is that the violation of the right to privacy does not harm the deceased.

In the sense of the application of the right to be forgotten, the EU case law is generally not conditioned by the presence or absence of damage to the data subject. It seems that the main purpose of the right to be forgotten is still to guarantee "the right not to be a victim of harm".

Eternal memory in the truest sense of the word, however, does not exclude the fact that the personal data of the deceased, which are freely available on the Internet, cannot lose their social significance in the process of changing life circumstances, or contain incomplete, inaccurate, unreliable or reliable, but defamatory or offensive information. In this case, if the publication and disclosure of such information on the Internet took place in an EU Member State whose legislation does not contain specific rules on the posthumous processing and protection of personal data, the person's memory and information identity will be distorted and violated.

The justification of the right to be forgotten through the protection of human dignity allows us to get out of the situation of the “lack of validity” of the right to be forgotten.

The concept of the right to be forgotten through the protection of human dignity reveals important aspects that go beyond simple "oblivion" in the digital age. The idea of preserving the dignity of a person after his/her death is reflected in the understanding of the concept of "digital remains". They are integral parts of our digital lives, representing aspects of personality that continue to exist even after a person’s death. In this context, the attitude towards "digital remains" requires respect and protection, like respect for the person himself/herself for his/her dignity.

The principle of preserving human dignity is also present in Article 1 of the CFR. Thus, the application of the right to be forgotten in the context of human dignity implies broader protection not only of the person during life, but also the preservation of his/her integrity after leaving this world. This calls for an ethical approach to the treatment of digital heritage based on respect for the inviolability of the human person and his/her dignity, which remains after death.

The "right to be forgotten" acts as an important counterweight to digital memory. Since people now have the opportunity to intervene in the future using their digital data, it is obvious that the simplest solution is that they will automatically provide the opportunity to anticipate

this situation. Staying in the logic of memorisation and constant accumulation of information can violate the reputation, dignity, privacy of the individual, as well as desecrate his/her memory after death.

Next, the "Streisand effect" is considered as an unwanted paradox of right to be forgotten. Despite the fact that the CJEU itself is gradually outlining the contours of the right to be forgotten, nevertheless, it also turns this right into a tool unsuitable for protecting human privacy in the digital world. The problem lies in the very wording that the CJEU uses in its judgments concerning the right to be forgotten. The CJEU itself explicitly indicates the information that the data subject tried to hide from third parties when applying to the CJEU in order to protect his/her privacy and reputation. This phenomenon is called the "Streisand effect". Consequently, courts, including the CJEU, should be careful when describing the factual circumstances of the case in question, in order to prevent not only violations of human privacy and reputation, as in the case of *Google Spain* through the "Costeja paradox", but also to prevent the use of the right to be forgotten for PR purposes.

Considering the scope of the right to be forgotten through the prism of the case law of CJEU, I come to the conclusion that the practice of the CJEU has left open the question of the territorial scope of the GDPR itself. From the EU's point of view, extraterritorial enforcement of the digital rights, in particular the right to be forgotten, is seen as a way to guarantee full protection of human rights.

However, developing rules to protect digital privacy in the context of balancing two approaches - local and global - instead of choosing one of them may be the best way to ensure that privacy remains a protected right even in the digital age. The interpretation of the *Google v. CNIL* decision as limiting the territorial scope of the right to be forgotten cannot be considered correct. Rather, it is the first attempt to balance the local and global application of the right to be forgotten. Having studied the case law of the CJEU, I come to the conclusion that the Court is faced not with a choice between local and global application of the right to be forgotten, but rather with the need to develop criteria that would help regulate the application of the EU data protection legislation outside the EU borders. I think it should be noted that some of the texts mentioned in this chapter have already been published in the scientific journals specified in the section belov.

In conclusion, the main outcomes drawn during the research are summarised and the necessary recommendations are given for the further development of the right to be forgotten.

1.6 Presentation of the thesis results

An essential requirement of doctoral studies is the presentation of research results, and the condition for the acceptance and defence of the thesis is the publication of its key parts. I have been studying innovations in the development of EU digital law, in particular the right to be forgotten, for several years and the results of my research have been presented in a number of active speeches at conferences not only in the Czech Republic, but also abroad (Belgium, Estonia). As part of my publishing activities, I have proposed separate sub-questions and more complex treatises in the following scientific papers and chapters, published in the Czech Republic and abroad:

Papers in scientific journals:

- HAMUĽÁK, Ondrej; KOCHARYAN, Hovsep; KERIKMÄE, Tanel. The Contemporary Issues of Post-Mortem Personal Data Protection in the EU after GDPR entering into Force. *Czech Yearbook of Public and Private International Law*, 2020, Vol. 11, pp. 225–238.
- HAMUĽÁK, Ondrej; KOCHARYAN, Hovsep; KERIKMÄE, Tanel; MUURSEPP, Peeter. Legal Person or Agenthood of Artificial Intelligence Technologies. Acta Baltica Historiae et Philosophiae Scientiarum, 2020, vol.8, No. 2, pp. 73–92.
- KOCHARYAN, Hovsep; HAMUĽÁK, Ondrej; KISS, Lilla Nóra, GABRIS, Tomáš. This Content is not Available in Your Country". A General Summary on Geo-Blocking in and outside the European Union. *International and Comparative Law Review*, 2020, Vol. 21, No. 1, pp. 153–183.
- KOCHARYAN, Hovsep; HAMUĽÁK, Ondrej; VARDANYAN, Lusine. The Global Reach of the Right to be Forgotten through the Lenses of the Court of Justice of the European Union. *Czech Yearbook of Public & Private International Law*, 2021, Vol. 11, pp. 196–211.
- KOCHARYAN, Hovsep; HAMUĽÁK, Ondrej; VARDANYAN, Lusine, KERIKMÄE, Tanel. Critical Views on the Right to be Forgotten after the Entry into Force of the GDPR: Is it Able to Effectively Ensure our Privacy? *International and Comparative Law Review*, 2021, Vol. 21, No. 2, pp. 96–115.
- KOCHARYAN, Hovsep; VARDANYAN, Lusine. The GDPR and the DGA proposal: are they in controversial relationship? *European Studies. The Review of European Law, Economics and Politics*, 2022, Vol. 9, No. 1, pp. 91-109.

- KOCHARYAN, Hovsep; STEHLIK, Vaclav; VARDANYAN, Lusine. Digital integrity: the foundation for digital rights and the new manifestation of human dignity. *TalTech Journal of European Studies*, 2022, Vol. 12, No. 1, pp.160-185.
- KOCHARYAN, Hovsep; HAMUĽÁK, Ondrej; VARDANYAN, Lusine. The Right to be Remembered?: The Contemporary Challenges of the "Streisand Effect" in t*he European Judicial Reality. International and Comparative Law Review*, 2022, Vol.22, No.2, pp.105-120.
- KOCHARYAN, Hovsep; VARDANYAN, Lusine. Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: main obstacles and challenges. *European Studies*, 2022, Vol. 9, No, 2, pp. 110-132.
- KOCHARYAN, Hovsep; VARDANYAN, Lusine. The right to data protection in the light of personality rights: does it prevent the emergence of data ownership? *Journal of Ethics and Legal Technologies*, 2022, Vol. 4, No. 1, pp.105-120.

Chapters in scholarly books:

- VARDANYAN, Lusine; HAMUĽÁK, Ondrej; KOCHARYAN, Hovsep; KERIKMÄE, Tanel. The Digital Sovereignty of the EU – Marking Borders in the Digital World? In TROITIÑO, David Ramiro; KERIKMÄE, Tanel; HAMUĽÁK, Ondrej (eds.). *Digital development of the European Union.* Springer International Publishing, 2023, pp. 196–211.

2 Privacy in digital society: concepts and new foundations

2.1 Privacy: A Brief History

As it is known, when analysing the right to be forgotten, we almost always intuitively slip into the sphere of protection of privacy and personality. And this is not accidental, because often the justification for the emergence and development of this right is considered to be the protection of privacy, especially if we take into account that the concept of privacy is associated with the level of development of technology and its use in everyday life. In sum, privacy is a dynamic concept with a tendency towards constant transformation. Reconfiguration of the elements underlying the understanding of privacy has occurred continuously and new combinations of technologies, meanings and practices have resulted in shifting boundaries between what is considered public or private space. Thus, privacy should be understood as an indicator of the relationship between the individual and society in accordance with the vectors of time, space and culture. This juxtaposition between privacy protection and technological development can be seen as early as 1939 in the USA. The US Supreme Court has made two judicial decisions in the *Weiss v. United States* and *Nardone v. United States*, where, through the interpretation of the Fourth Amendment of the US Constitution (which is one of the first attempts to formalise the protection of private space and personal autonomy), it refuted the evidence obtained as a result of illegal wiretapping.[14]

During the 20th century, the right to privacy acquired the status of a human right. As a universal right, privacy is enshrined in Article 12 of the UN Universal Declaration of Human Rights (1948),[15] as well as in Article 17 of the International Covenant on Civil and Political Rights (1966).[16] The wording and structure of both provisions are very similar and the latter legal document was designed from the outset to be legally binding on states in order to protect the rights of individuals.[17] It was a novel entry into the human right catalogue and had been originated in a somewhat accidental manner due to the absence of any predecessors in state

[14] Judgment of the Supreme Court of 11th December 1939, file No. 308 U.S. 321; See also Judgment of the Supreme Court of 11th December 1939, file No. 308 U.S. 338.
[15] United Nations General Assembly. The Universal Declaration of Human Rights (UDHR). New York: United Nations General Assembly, 1948.
[16] International Covenant on Civil and Political Rights (adopted 19 December 1966, entered into force 23 March 1976) 999 UNTS 171, Article 17.
[17] JOSEPH, Sarah, CASTAN, Melissa. *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary.* Oxford: Oxford University Press, 2013, 1042 p.

constitutions or basic laws. The potential of this right was dramatically underestimated at the time of its creation,[18] and since then it has become one of the most important human rights.

At the European level, the European Convention on Human Rights (1950) was adopted, which also enshrined the right in question. Moreover, the case law of the ECtHR has formulated the basic contours of this right and contributed to its development, including taking into account the degree of technological development.[19] Since the early 1960s, with the increasing use of large-scale computing systems, there has been an increased focus on controlling the dissemination of data. This led to increased demands for transparency and accountability in the handling of personal information. In response to technological change in the 1970s, the European countries developed an approach to regulation that was not limited to particular sectors. It was an "integrated approach" that was not tied to a particular industry.[20] The first data protection mechanisms were implemented in Germany (law in Hesse (1970)) and Sweden (the world's first national data protection law (1973)).[21]

Given the diversity of legislation in European countries, there has been a need to harmonise regulatory frameworks to ensure their compatibility. In 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[22] provided specific rules for the protection of personal data.[23] This instrument is the only legally binding international agreement on data protection. It was revised in May 2018 and its modernised version (Convention 108+)[24] was intended to provide a basis for the development of more multilateral approaches to regulation and governance in this area.[25] The Convention 108+ contains key principles governing the collection, storage and processing of personal data,

---

[18] DIGGELMANN, Oliver, CLEIS, Maria Nicole. How the Right to Privacy Became a Human Right, Human Rights Law Review, 2014, vol. 14, No. 3, pp. 441–458.

[19] ALLEGRI, Maria Romana. The Right to be Forgotten in the Digital Age. In COMUNELLO, Francesca et al. (eds.) *What People Leave Behind. Frontiers in Sociology and Social Research*. Springer, Cham, Vol 7., 2022, pp. 237-251.

[20] HOOFNAGLE, Chris Jay et. al. The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, 2019, vol. 28 No. 1, pp. 69-72.

[21] See GSTREIN, Oskar; BEAULIEU Anne. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philos. Technol, 2022, vol. 35, No. 3, pp. 43–44.

[22] Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981).

23 DALLA CORTE, Lorenzo. *Safeguarding data protection in an open data world: On the idea of balancing open data and data protection in the development of the smart city environment and data protection in the development of the smart city environment*. Tilburg: Tilburg University, 2020, 125 p.

[24] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), 128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018)

[25] See KWASNY, Tatjana, et. al. Towards reduced meat consumption: A systematic literature review of intervention effectiveness, 2001–2019. *Appetite*, 2022, vol. 168, 17 p.

developed in more detail and including individual rights and obligations for those collecting and using personal data.

In the EU, the DPD (1995)[26] was adopted, which enshrined similar principles to those, specified in the Convention 108+. However, a significant impetus for addressing privacy protection at the regional level has been the adoption of the CFR and the GDPR, as well as the judicial activism of the CJEU in this area. The GDPR as an offshoot of the Convention 108+ includes, among others, some additional rights, such as the right to erasure or "the right to be forgotten", the right to data portability and the right not to be subject to decisions that were made solely by automated means. The GDPR emphasizes privacy and data protection as two interrelated but completely independent human rights. Data protection has thus become one of the main approaches to regulating privacy and confidentiality protection in EU law.

2.2 Doctrinal approaches to the concept of privacy

The concept of the right to privacy is so specific and multi-layered that it is impossible to describe and define it in details, especially when it encompasses a significant number of aspects relating to the psychological and physical integrity of the individual and his/her privacy in the interaction of social relations.[27] The term "privacy" is also not defined in the legal doctrine, European law or international covenants. As J. J. Thomson points out that: "[p]erhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is".[28] Such a remarkable feature lies in the fact that, being an almost indefinite legal category, privacy makes it possible to be widely used in various situations, including those arising from the rapid development and introduction of technologies, while not limiting the application of the law or weakening human protection. This uncertainty has led to a situation where various conceptions of privacy have emerged in the doctrine of law, which can be grouped according to the following ontological categories:

1. *The concept of privacy as a right to be left alone:* this concept was discussed by Samuel D. Warren and Louis D. Brandeis.[29] The authors saw its development as an inevitable

[26] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[27] ECtHR: Judgment of Grand Chamber of 4th December 2008. *S. and Marper v. The United Kingdom*. Nos. 30562/04 and 30566/04.
[28] THOMSON, Judith Jarvis. *The Right to Privacy. Philosophy and public affairs.* Princeton, N.J: Princeton University Press, 1975, Vol. 4, No. 4, pp. 295-314.
[29] WARREN, Samuel D.; BRANDEIS, Louis D. Right to privacy. Harvard Law Review, 1890, vol. 4, No. 5., pp. 193-220.

step in the development of society. They defined it as a right to essentially protect one's "inviolate personality" from intrusion or unwanted revelation.[30] Such a "negative" right protected the individual primarily from state authorities.

2. *The reductionist concept of privacy:* the concept reduces privacy to a group of other fundamental interests. The concept does not contemplate the possibility of such a separate right. J. J. Thomson notes that privacy is contrary to individual diverse interests in the sense that any interference with privacy can be interpreted as interference with some of the more fundamental rights of the individual, while the right to privacy as such should not be affected.[31] A critique of this approach is given by T. Scanlon, who argues that: "[a]s far as I can see I have no such general rights to begin with. I have an *interest* in not being looked at when I wish not to be, and I may have a similar interest with respect to certain objects. But rights directly corresponding to these interests would be too broad to form part of a workable system".[32]
3. *The concept of privacy as access to a person:* Privacy is defined as the state of being protected in various ways from unwanted intrusion by others. This broad definition encompasses the full range of meanings of privacy. S. Bock defines privacy as the "condition of being protected from unwanted access by others – physical access, personal information, or attention".[33] Privacy statements are statements about controlling access. A. Allen suggests that "privacy refers to a degree of inaccessibility of a person or information about her to others' five senses and surveillance devices".[34] R. Gavison writes that "(…) an individual enjoys perfect privacy when he is completely inaccessible to others".[35] However, the approach does not stand up to criticism. A.F. Westin cites the example of solitary confinement as an example of "too much" privacy.[36] This critique shows the peculiarity of privacy as an interpersonal phenomenon.
4. *The concept of privacy as access control over private information:* The concept considers privacy as a requirement for individuals, groups, or institutions to determine

---

[30] Ibid.
[31] THOMSON, Judith Jarvis. *The Right to Privacy. Philosophy and Public Affairs,* Princeton, N.J: Princeton University Press, 1975, vol. 4, No. 4. pp. 295-314.
[32] SCANLON, Thomas. Thomson on Privacy, Philosophy and Public Affairs, 1975, vol. 4, No. 4, pp. 315-322.
[33] BOK, Sissela. *Secrets: On the Ethics of Concealment and Revelation*, Pantheon. New York: Oxford University Press, 1983, 332 p.
[34] ALLEN, Anita, L. Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm Commentary. Connecticut Law Review, 2000, vol. 32, No. 3, p. 867.
[35] GAVISON, Ruth. Privacy and the Limits of Law. Yale Law Journal. 1980, vol. 89, No. 3, p. 428.
[36] WESTIN, Alan F., *Privacy and Freedom*, New York: Atheneum, 1967, 487 p.

for themselves when, how, and to what extent information about them is shared with others. Viewed from the point of view of an individual's attitude to social participation, privacy is the voluntary and temporary withdrawal of a person from society as a whole by physical or psychological means, either in a state of solitude or intimacy with a small group, or, being among large groups, in a state of anonymity or restraint. [37] Other people's knowledge of us shapes how we can present ourselves and act towards others. This form of confidentiality is relevant, first of all, in friendship and love relationships and serves as both protection of the relationship and protection within the relationship. In this concept, this actually constitutes the very essence of privacy in the form of "relative privacy", which guarantees the possibilities of detachment that form the basis of authentic life.[38]

5. *Cluster privacy concepts:* According to this approach, privacy is a certain comprehensive set of different aspects. According to Judith DeSue, the "cluster concept" emphasizes the links between different interests without reducing privacy to them: “I argue that privacy is best understood as a cluster concept covering multiple privacy interests, including those enhancing control over information and our need for independence as well as those enhancing our ability to be self-expressible and to form social relationships”. [39] The author defines three aspects of privacy: 1) informational privacy, 2) accessibility privacy and 3) expressive privacy.[40] The protection of privacy in relation to these three dimensions is also crucial for democratic decision-making procedures.[41]
6. *The concept of privacy as a right to the information flow of personal information (Contextual Integrity):* In this innovative concept H. Nissenbaum, refusing to provide a single definition of privacy[42] proposes to understand the right to privacy as "the right to an appropriate flow of personal information".[43] As a rule, this flow is governed by context-dependent information norms. They are characterized by four parameters:

---

[37] Ibid.
[38] FRIED, Charles. Privacy. The Yale Law Journal, 1968, vol. 77, No. 3, pp. 475-493.
[39] DECEW, Judith Wagner, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca, New York: Cornell University Press, 1997, 199 p.
[40] BORKOWSKI, Susan, DECEW, Judith Wagner, In Pursuit of Privacy: Law, Ethics and the Rise of Technology. Teaching Business Ethics, 1999, vol. 3, No. 4, pp. 402–406.
[41] ROBERTS, Huw. Informational Privacy with Chinese Characteristics. In MÖKANDER, Jakob, ZIOSI, Marta (eds.). The 2021 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook. Springer, Cham., 2022, pp. 9-23.
[42] NISSENBAUM, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford: Stanford University Press, 2009. 304, p.
[43] Ibid., p.127

specific contexts, actors, types of information, and (importantly) principles of transmission.[44] The transfer principle is "restricting the flow of information from party to party in context".[45] What is considered private information depends on the different norms imposed on the flow of information governing different social contexts, such as the contexts of education, religion, security, or politics (the "contextual integrity" of various contexts).[46] The principle of adequate transfer may, depending on the information norm, in some contexts be understood as controlling access of the individuals involved. In this sense, H. Nissenbaum does not strictly oppose control-access approaches, although she advocates their limited use within the general framework of information privacy. The concept does not focus on the rights and duties of individuals, but more on personal privacy, which can serve as a basis for individual autonomy and dignity, as required by international human rights law. Many existing interpretations of the right to privacy have already been adapted to specific contexts, such as criminal procedures.[47]

When considering privacy in the context of the digital age, in my opinion the concept of social privacy cannot be avoided. A.F. Westin defines four states of privacy: "*Solitude* is being free from observation by others. *Intimacy* refers to small group seclusion for members to achieve a close, relaxed, frank relationship. *Anonymity* refers to freedom from identification and from surveillance in public places and for public acts. *Reserve* is based on a desire to limit disclosures to others; it requires others to recognize and respect that desire".[48]

States of privacy mentioned above explain how privacy operates and their foundation is based on social norms and legal traditions. According to A.F. Westin, privacy is linked to secrecy, however, he does not give a clear definition of secrecy. In sum, he argues that privacy and secrecy are related, even though he admits that this relationship lacks clarity, but the relationship itself is relevant. Of course, Westin's concept needs to be rethought in the light of new realities in the aspect that, as De Terwangne points out, privacy (on the Internet) should not be understood as intimacy or secrecy.[49] Rather, it refers to another dimension of privacy,

[44] Ibid., pp. 140-141
[45] Ibid., p.145
[46] Ibid., pp. 127-231
[47] SELBST, Andrew D. Contextual Expectations of Privacy. Cardozo Law Review, 2013, Vol. 35, No. 2, pp. 699–705.
[48] WESTIN, Alan F., *Privacy and Freedom*. New York: Atheneum, 1967, 40 p.
[49] DE TERWANGNE, Cecile. Internet privacy and the right to be forgotten/right to oblivion. *Revista de Internet, derecho y politica*, 2012, Vol. 13, pp. 31-43.

i.e. individual autonomy, the ability to make choices, make informed decisions, etc. In the context of the Internet, this dimension of privacy refers to informational autonomy or informational self-determination.[50]

However, the most distinctive feature of Westin's concept of privacy is that:

a) privacy is a right, and
b) it is the right of individuals, groups or organizations to make discretionary decisions about when, how and to what extent their personal information will be disclosed to others.[51]

As A. F. Westin writes: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve".[52] This concept has the advantage that the discussion on the right to be forgotten also covers aspects relevant to groups and organizations.

The idea that Big Data analysis technologies are aimed at the group level is also proposed by other researchers. L. Floridi suggests considering group privacy to overcome ethical approaches that are either too focused on individuals or atomistic agents.[53] The idea is that if rights are formulated at the group level, this can help to address the deficiencies in the regulation of individual rights that prevent people from developing and shaping a dignified existence. [54] Groups respond to data processing through self-organisation and become significant players interested in decision-making processes. Many types of harm, especially those related to the use of algorithmically controlled systems, are not directly related to the data subject. Typically, individual source data is first aggregated, then analysed and reinterpreted before being put into action.[55] Despite the fact that EU legislation grants certain rights to

[50] Ibid.
[51] WESTIN, Alan F., *Privacy and Freedom*. New York: Atheneum, 1967, 35 p.
[52] Ibid.
[53] FLORIDI, Luciano. The fourth revolution: how the infosphere is reshaping human reality. Oxford: Oxford University Press. 2014, 248 p.
[54] VAN DER SLOOT, Bart. Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR. In TAYLOR, Linnet, FLORIDI, Luciano, VAN DER SLOOT, Bart (eds.), *Group Privacy: New Challenges of Data Technologies*. Springer International Publishing, 2017, pp. 197–224.
[55] Ibid., pp. 215-223.

individuals, it is doubtful that the emphasis on individual control remains effective in the era of Big Data, when it is becoming increasingly difficult to keep abreast of every data processing operation.[56] Because "individual control is too narrow" in the context of Big Data, group privacy protection (in A.F. Westin's terminology - "relationship privacy") is required. "Data is analysed based on patterns and group profiles".[57]

L.T. Taylor, L. Floridi and B. van der Sloot present different ways of defining the group, but with a focus on technology and the right to be forgotten, their approach sees the digitally defined group as the most appropriate.[58]

However, many problems arise when trying to implement group privacy. It is difficult to understand how a group should be organized or how to effectively integrate its rights into decision-making processes? Nevertheless, such an epistemological shift requires a new approach to privacy and data protection, including the right to be forgotten, although the approach is mainly limited to the academic sphere. Nevertheless, the possibility of its legal application is also not excluded, as discussed below.

Thus, it can be seen that privacy concepts are beginning to be considered primarily in relation to the processing of information and the possibility of controlling the dissemination of information. Data processing does not negate existing privacy grounds, but adds new ones on which new privacy concepts are built.

While traditionally privacy interests were implicit in the legal or social protection of personal property and space, intimate surroundings or personal effects,[59] the contemporary concepts of privacy are closely linked to technological developments that allow for new intrusions into the intimate aspects of life. Digital technologies, including databases, the Internet and so on, call for a further evolution of privacy rights, both conceptually and legislatively.[60]

2.3 Privacy, Digitalisation, Data Protection

Every society in the modern world is based on the exchange of personal data, and thus data protection is more related to the rules of their transfer and use, as well as the control and

[56] Ibid.
[57] Ibid.
[58] Ibid.
[59] DEVRIES, Will Thomas. Protecting Privacy in the Digital Age. *Berkeley Technology Law Journal.* 2003, Vol. 18, p. 283.
[60] Ibid.

authority of individuals to make decisions regarding their own personal information.[61] However, as A. Rengel points out: "Individuals have little ability to control this collection or manipulation of their data".[62] Technologies enables invisible data processing, increasing the opportunities for sharing and collecting information, making it difficult to assess by whom, when and what information was collected and whether the collection process was legitimate. The possibilities for data collection and processing are further enhanced by the introduction of the Internet of Things ("IoT") and the Internet of Bodies ("IoB"). This gives rise to privacy risks, the nature of which is explained by K. Huckvale, J. Torous, and M.E. Larsen.[63] With the increasing collection of data, some researchers have even sought to move away from an understanding of privacy based on notions of information control or secrecy.

Among the privacy risks of datafication, the separation of public and private sector regulation of data processes is becoming increasingly complex. The proliferation of data is blurring the boundaries between citizens and consumers as more public services begin to rely on platforms provided by corporations, "raising concerns both about individual and collective autonomy/sovereignty".[64] F. Brunton and H. Nissenbaum point out that information gathering occurs in asymmetric power relations: we rarely have a choice about whether or not we are controlled, what to do with any information collected, or what is done to us based on conclusions drawn from that information.[65] The destruction of privacy as a result of data collection and processing increases the ability of large technology companies and governments to influence the people whose data is collected.[66] This indicates the connection between privacy and power.

Another consequence of the impact of datafication on everyday life is the spread of surveillance. Many authors, analysing the "surveillance state", discuss various social contexts in which violations of information confidentiality can interact with restrictions on freedom. Sh. Zuboff conducts a critique of surveillance capitalism and the "instrumental power" of this state,

---

[61] SCHÜNEMANN, Wolf J., BAUMANN, Max-Otto. Privacy, data protection and cybersecurity in Europe. *New York, NY: Springer International Publishing*, 2017, 145 p.
[62] RENGEL, Alexandra. Privacy-Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights. *Intercultural Human Rights Law Review*. 2013, Vol. 8, pp. 177 – 230.
[63] HUCKVALE, Kit, et al. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Network Open*, Vol. 2, No. 4, 2019, p. 10.
[64] VEALE, Michael. Sovereignty, privacy and contact tracing protocols. Data Justice and COVID-19: Global Perspectives. In: TAYLOR, Linnet et. al. (eds.) Data Justice and COVID-19: Global Perspectives. London: Meatspace Press. 2020. pp. 34–39.
[65] BRUNTON Finn, NISSENBAUM, Helen, Obfuscation: A User's Guide for Privacy and Protest, Cambridge, MA: MIT Press. 2015, 49 p.
[66] VELIZ, Carissa. Privacy is Power: Why and How You Should Take Back Control of Your Data, London: Bantam Press. 2021, 224 p.

where privacy is seen as data and a commodity that can be sold.[67] She opposes the process of turning personal life into behavioural data and commercial products: personal data should not be considered as a commodity, since they represent human experience. Some scholars use the term "data colonialism", which emphasizes the constant operational impact inherent in the datafication process.[68] The term "data colonialism" reflects a new form of colonialism involving the exploitation of human lives.

Another dilemma is the freedom to create an actual personality and the danger of the permanence of information. People are "social animals" who have an urgent need to communicate with other people.[69] Datafication has provided the most accessible means of communication, but people have to give up their privacy to a certain extent by making a deal and their data for "free" services. This happens voluntarily in the pursuit of a full-fledged social life, but limits the protection of personal data.[70] Emphasising the "privacy paradox", E. Hargittai and A. Marwick argue that although people are aware of the dangers of sharing information online, they feel they should "acknowledge that individuals exist in social contexts where others can and do violate their privacy".[71] In addition, the risk to privacy may be caused by the "social cost of a reduced presence online".[72]

However, it is not always the individual who chooses his or her own presence on the Internet. Nor does refusing to use the Internet help to prevent the collection and processing of personal data. Data generated in highly connected environments allow the collection of data not only on individuals who consent to its collection and use, but also on those who have not given such consent. Sharing the same time, space and cultural dimension makes it difficult for an individual to be isolated, especially if the social architecture does not allow such an objection.[73]

---

[67] ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019,

[68] CIESLIK, Katarzyna, MARGÓCSY Dániel. Datafication, Power and Control in Development: A Historical Perspective on the Perils and Longevity of Data. Progress in Development Studies, Vol. 22, No. 4, 2022, pp. 352–373; KWET, Michael. 'Digital Colonialism: US Empire and the New Imperialism in the Global South'. Race and Class, Vol. 60, No., 2019, pp. 3–26.

[69] ACQUISTI, Alessandro, et al. Privacy and human behavior in the age of information. *Science,* Vol. 347, No. 6221, 2015, p. 510.

[70] SCHÜNEMANN, Wolf J., BAUMANN, Max-Otto. Privacy, data protection and cybersecurity in Europe. New York, NY: Springer International Publishing, 2017, 145 p.

[71] HARGITTAI, Eszter, MARWICK, Alice. 'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, Vol. 10, 2016, pp. 3737–3757.

[72] PAPACHARISSI, Zizi, GIBSON, Paige L.. Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites., In TREPTE, Sabine, REINECKE, Leonard (eds.). *Privacy Online.* Springer Berlin Heidelberg, 2011, pp. 75–89

[73] CANNATACI, Joseph A., et. al. Privacy, free expression and transparency: Redefining their new boundaries in the digital age. *Unesco Publishing*, 2016, 142 p.

Content on the Internet does not have a natural expiration of time and people face their past for a long time, because they cannot completely change their digital footprints. As S. Alessi righty argues: "Once information is uploaded, the Internet stores it permanently, in what has been called "digital eternity." Hence, when personal information is uploaded online, our most embarrassing or painful moments may acquire lasting significance and haunt our lives. The Internet is an integral part of our lives to collect information, manage finances, socialize, and shop. Thus, it risks infringing upon individuals' right to privacy".[74] Such long-term information can indicate an individual's interpersonal relationships and his/her social status.

Digital technologies take away from us our natural right to make a mistake (even unintentional), and often such digital technologies become a "weapon" against ourselves, for example, through news websites, forums and/or other social networks (for example, Facebook, Instagram, Twitter, etc.).[75] In such conditions, when digital technologies are rapidly developing, we willy-nilly become "perpetual slaves" of what we ourselves have said and/or done, or what third parties have told us and/or done. Of course, this phenomenon also existed before the development of digital technologies, but in the "offline" world information did not have such a wide and cross-border availability as it is nowadays. Moreover, in the "offline" world even the most up-to-date information was usually subjected to moral aging and was often forgotten after a certain period of time. This is precisely the socio-psychological prerequisites for the formation and development of the right to be forgotten: it strives to become a "lifeline" for human privacy and reputation in the conditions of the "unforgettable" Internet, however it faces various obstacles on its way, which negates its privacy-protective potential.

The combination of the constant nature of information and the functioning of online search engines, as well as the algorithms of online search engines often lead to links to unflattering information or images about the data subject on the first pages. It turns out that information can already be stored, displayed and/or processed perpetually by third parties (even those we may not know about), which in turn infringes on the privacy and dignity of a person in the digital world. It seems to me that, in legal terms, protecting the individual in the digital sphere in the context of datafication involves resolving the freedom-security dilemma. As A.R.

---

[74] ALESSI, Stefania. Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation. Emory International Law Review, 2017, Vol. 32, no. 1, pp. 145–171.

[75] For example, in the case of *Einarson v. Iceland* (Application No. 24703/15, Judgment Strasbourg 7 November 2017, Final 07/02/2018) the ECtHR held that the publication of a photo on Instagram violated article 8 of the ECHR (i.e. the right to respect for private life), since a published photo on a publicly accessible website may reach a large number of Internet users).

Servent argues, the European courts will now have to balance security and freedom as fundamental rights.[76]

Among the mechanisms for mitigating the above-mentioned risks of confidentiality in conditions of datafication and extensive collection of information, the right to be forgotten occupies a special place. The emergence of the phenomenon of the right to be forgotten in the EU's legal reality can clearly be considered as a step forward in question of ensuring the privacy protection of the data subject, giving him/her a *carte blanche* to protect his/her privacy in conditions when "the Internet never forgets".[77] In turn, V. Reding argues that the Internet has virtually unlimited data search and storage capabilities. Thus, even small fragments of personal data can become a big hit, even after a long time has passed since they were made public.[78] The right to be forgotten in the GDPR is based on existing rules to better manage the risks of data protection on the Internet. H. Torop considers the right to be forgotten as the right to make a mistake: the Internet was created in order to constantly store our "digital footprints" and this requires the realization of new rights, among which is the right to be forgotten, which acquires special value.[79] Thus, the right to be forgotten becomes one of the main mechanisms for preventing potential damage to human rights and his/her personality in the context of the datafication of society.

---

[76] See SCHÜNEMANN, Wolf J., BAUMANN, Max-Otto. Privacy, data protection and cybersecurity in Europe. *New York, NY: Springer International Publishing*, 2017, 145 p.

[77] CROCKETT, May. The Internet (Never) Forgets. *Science and technology Law Review*. 2017, Vol. 12, No. 2., pp. 151 – 181.

[78] REDING, Viviane. The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age. *SPEECH/12/26* [online]. 22th January 2012. [cit. On. 25th December 2023]. Accessible at:
< https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26>.

[79] TOROP, Henri. Õigus olla unustatud - kas rahvusvaheliselt tunnustatud inimõigus? Avaliku õiguse osakond. *Tartu: Magistritöö*, 2018. 98 p.

3 Introducing the right to be forgotten

3.1 The essence and justification of the right to be forgotten

The right to be forgotten cannot be considered an entirely new right. In France *droit à l'oubli* has been recognized since the 1960s. In the judicial practice of the USA, this right has already been found in the 1970s, starting with the case of *Briscoe v. Reader's Digest Association*.[80] From the very beginning, the idea of the right to be forgotten is based on the desire to provide an effective remedy for the "criminal past". As A. Mantelero notes, historically, the right to be forgotten arises from the need "of an individual to determine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past".[81] The right to be forgotten in this case has the justification of privacy as a fundamental right, the goal of which is to avoid possible damage that may be caused to the reputation of the individual.[82] J.V.J. Van Haboken also speaks of such a fundamental connection.[83]

The same rationale for the right to be forgotten can be seen in the case law of the ECtHR, where the right to be forgotten is included within the scope of Article 8 and is essentially the result of judicial activism. Being a relative right, it is subject to a number of restrictions "in accordance with the law" and on what is "necessary in a democratic society in the interests of national security and public safety" and so on.

EU law enshrines the right to data protection as an independent right in EU primary law (in Article 16(1) of the TFEU and Article 8(1) of the CFR) and in the case law of the CJEU.[84]

---

[80] Judgment of the Supreme Court of California, *Briscoe v. Reader's Digest Association, Inc.,* L.A. No. 29813 [4 Cal.3d 529, 93 Cal. Rptr. 866, 483 P.2d 34]. (Cal. 1971).

[81] MANTELERO, Alessandro. The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'. *Computer Law and Security Review*. 2013, Vol. 29, No. 3, pp. 229–235.

[82] JONES, Meg Leta, AUSLOOS, Jef. The Right to Be Forgotten Across the Pond. *Journal of Information Policy*, Vol. 3, 2013, pp. 1-23.

[83] VAN HOBOKEN, Joris V. J.. The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember. Freedom of Expression Safeguards in a Converging Information Environment. Prepared for the European Commission Appointment Letter No. 25797. [online]. 14th January 2013. [cit. on 25th December 2023]. Accessible at: <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC86747/lbna26410enn.pdf>.

[84] Court of Justice of the European Union: judgment of the 20th May 2003. *Rechnungshof (C-465/00) v. Österreichischer Rundfunk and Others and ChristaNeukomm (C-138/01) and Joseph Lauermann (C-139/01) v. ÖsterreichischerRundfunk* [2003], Joined cases C-465/00, C-138/01 and C-139/01,ECLI:EU:C:2003:294; Court of Justice of the European Union: judgment of the 11th November 2014. *František Ryneš v. Úřad pro ochranu osobních údajů* [2014], Case C212/13; ECLI:EU:C:2014:2428; Court of Justice of the European Union: judgment of the 6th October 2015, *Maximillian Schrems v. Data Protection Commissioner* [2015], C-362/14, ECLI:EU:C:2015:650; Court of Justice of the European Union: judgment of 08th April 2014. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and NaturalResources and Others and Kärntner Landesregierung and Others* [2014], CJEU Joined cases, C-293/12 and C-594/12, ECLI:EU:C:2014:238.

The right to be forgotten has been given a new rationale, becoming a concretisation of the right to personal data protection. I. Falk-Pierrotin even notes that the right to be forgotten is simply the application of general data protection law to a search engine.[85] The CJEU has already in the *Google Spain* case invoked a new fundamental right to justify the right to be forgotten. The Court found that the data subject has a right under Articles 7 and 8 of the CFR to the right to be forgotten as a right to request that information is made no longer available to the general public by removing the list from the results returned by a search performed by a link to the data subject's name.[86]

Recognising the protection of personal data as a fundamental right takes it beyond the general protection of privacy. However, according to the case law of the CJEU, fundamental rights are considered to be general principles deriving from constitutional traditions common to member States and from international human rights agreements.[87] It is impossible to find such a common basis for the right to data protection in constitutional traditions, since the constitutional traditions of the EU member States base the right to data protection on completely different values. This means that the right to data protection as an independent fundamental right does not have a clear and defined legal basis or justifications like other fundamental rights.

First of all, "economic logic" led to the constitutionalisation of data protection: modernity is fuelled by "data", which C. Humby called the "new oil".[88] As M.L. Jones notes, giving personal data protection such a high rank in EU law related to the single market, which ignores privacy as a right and it protects economic freedoms, not the security of the individual.[89] In this case, the "economic" logic is aimed at protecting the economic benefits of data processing and at satisfying the public interest in access to information, however, the logic of "security" requires that the right to be forgotten be more related to ensuring the safety of citizens, rather than protecting individual freedoms and rights, focusing on the safety of the individual, rather than on democracy.[90] Thus, it is possible to discern the collective nature of this right.

---

[85] FALQUE-PERROTIN, Isabelle. Pour un droit au déréférencement Mondial. Debates du Monde. [online]. 12th January, 2017 [cit. on 25th December 2023]. Accessible at: <https://www.cnil.fr/fr/pourun-droit-au-dereferencement-mondial>.

[86] Exclusion from the list does not entail the complete removal of the link from the indexes of the search engine operator or the removal of information along the chain of controllers processing the information.

[87] See Judgment of the Court of 14 May 1974. *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities.* Case 4-73., para. 13.

[88] CHARLES, Arther. Tech giants may be huge, but nothing matches big data [online]. Guardian. 23th August 2013. [cit. on. 25th December 2023]. Accessible at: <http://www.theguardian.com/technology/2013/aug/23/tech-giants-data>

[89] JONES, Meg Leta. *Ctrl + Z: The right to be forgotten.* New York: New York University Press. 2016, 75 p.

[90] SCHÜNEMANN, Wolf J., BAUMANN, Max-Otto. Privacy, data protection and cybersecurity in Europe. *New York, NY: Springer International Publishing*, 2017, 145 p.

Nevertheless, the recognition of fundamentality did not solve the issue of individual protection and did not achieve the logic that led to its fundamentality. In cases *Schrems* and *Coty* the CJEU holds the view that the DPD (and now the GDPR) as a whole should be considered as an exercise of the fundamental right to data protection.[91] The provisions of the GDPR show one very remarkable feature: the right to personal data protection as a fundamental right is strikingly different from other fundamental rights: it protects the compromise between the rights and interests of data subjects and data controllers, including the interests of enterprises and the state in data processing, while almost all fundamental rights protect individual interests.[92] Thus, despite the fact that the right to be forgotten, as a concretisation of the fundamental right to data protection, should primarily regulate the relationship between the individual and the state, in the GDPR it becomes, in particular, one of the mechanisms for regulating the relationship between the private interests of the data controller (processor) and the data subject himself/herself. Moreover, the legal regulation proposed by the GDPR puts these private subjects in an unequal position from the very beginning. The data controller has a balancing duty between the data subject's request under Article 17(1) of the GDPR and the limitations outlined in Article 17(3) of the GDPR. This process is often referred to as the "notice-and-takedown" procedure. However, there are concerns about its alignment with Article 6 of the ECHR, particularly regarding the principle of "equality of arms" mentioned in Article 6(2) of the TFEU as a fundamental right within the EU. While data subjects have the option to challenge data controllers' decisions in national courts, there remains controversy over whether this procedure adequately safeguards the rights of data subjects and the broader public interest. In fact, the issues of ensuring and respecting the right to be forgotten are transferred to a private subject in the first instance, which raises serious concerns about the observance of this right with a huge economic interest in the data controller.

The mechanism of legal balancing delegated to enterprises, rather than to EU data processing authorities, makes rights to be forgotten a controversial right, which is a mechanism for establishing a balance between the data subject and the data processor, giving the data subject a limited right to participate (and very inefficiently) in the operations of processing his/her data. Assigning responsibility for balancing rights to data controllers and giving freedom

---

[91] See FUSTER, Gloria González, GELLERT, Raphaël. The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right. *International Review of Law, Computers amd Technology*. 2012, Vol. 26, No. 1, pp. 73–82.

[92] VAN DER SLOOT, Bart. Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR. In TAYLOR, Linnet, FLORIDI, Luciano, VAN DER SLOOT, Bart (eds.), *Group Privacy: New Challenges of Data Technologies*. Springer International Publishing, 2017, pp. 197–224.

of action when deciding whether data subjects will be allowed to exercise their right to be forgotten or not significantly reduces the law enforcement potential of the right in question.

As N. Purtova indicates: "(…) the adoption in April 2016 of the General Data Protection Regulation ('GDPR') marked the end of the European data protection reform and is a major development on a legislative level (…) which implied, among others, "that individuals are in control of their personal data and trust the digital environment." As a result, the GDPR contains new rights considered by some to be property-like, e.g. the rights to data portability and to erasure ('the right to be forgotten')".[93] The origins of the fundamental right are partly seen in the regulation of the market and the promotion of the free flow of information, which means that this right is more an instrument of market regulation than a classical fundamental right. Thus, the right to be forgotten as a concretisation of this fundamental right has the potential to be a mechanism for regulating the personal data market.

Some elements of the right to be forgotten can be traced in the concept of the right to information self-determination, which a number of researchers recognise as one of the conceptual foundations of the right to data protection, enshrined in Article 8 of the CFR,[94] despite the fact that this right does not exist in EU law, but is peculiar to German law.[95] The concept of information self-determination refers to the right and opportunity of each person to determine what information about him/her is disclosed to others and for what purposes such information can be used.[96] For some authors, it also provides full control over the use of personal data to the individual.[97] Recital 7 of the GDPR also states that "[n]atural persons should have control of their own personal data", so one can somewhat agree with those scholars who argue that the idea of information self-determination is the main reason for the

---

[93] PURTOVA, Nadezhda. Do property rights in personal data make sense after the big data turn: Individual control and transparency. *Journal of Law and Economic Regulation*, Vol. 10, No. 2, 2017, pp. 64–78.

[94] SCHMIDT, Bernd, Art. 1 DSGVO. In TAEGER, Jürgen, GABEL, Detlev (eds.), DSGVO BDSG, 3rd edition, *Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft*, 2019, 25 p.; KÜHLING, Jürgen, RAAB, Johannes. Einführung, In KÜHLING, Jürgen, BUCHNER, Benedikt (eds.), *Datenschutz-Grundverordnung BDSG Kommentar*, 3rd edition, C.H. Beck, 2020, 26 p.; See also: ROUVROY, Antoinette, POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development. In GUTWIRTH, Serge et al. (eds.), *Reinventing Data Protection*. Springer, 2009, 68 p.

[95] The German Federal Court (FCC), in its two 2019 judicial decisions on the "right to be forgotten," expanded information self-determination to include the commercial use of data by technology giants, since they limit the space of individual discretion and information self-determination. These court decisions extend information self-determination to a context limited to private individuals, which we partially see in the GDPR; See also: GSTREIN, Oskar Josef. Right to be forgotten: European data imperialism, national privilege, or universal human right? *Review of European Administrative Law (REALaw),* 2020, Vol. 1, pp. 136-139.

[96] SCHWARTZ, Paul M. Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology. *William and Mary Law Review*, Vol. 53, No. 2, 2011, p. 368; BAMBERGER, Kenneth A., MULLIGAN, Deirdre K.. Privacy in Europe: Initial Data on Governance Choices and Corporate Practices. *The George Washington Law Review*, Vol. 81, 2013, p. 1539.

[97] ROUVROY, Antoinette, POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development. In GUTWIRTH, Serge et al. (eds.), *Reinventing Data Protection*. Springer, 2009, 68 p.

GDPR.[98] The GDPR-rights, including the right to be forgotten, are to some extent based on the concept of information self-determination, however, it is impossible to exercise full control through these rights due to important limitations of the rights themselves provided for in the GDPR. Thus, the right to be forgotten can be exercised only if one of a limited set of situations is provided. Therefore, it is not possible to say that data subjects have a general right to request the deletion of their personal data or object to the processing of their personal data.

Special situations, such as when personal data is no longer needed in connection with the purpose for which they were collected (Article 17(1)(a) of the GDPR) or when the data subject withdraws consent and there is no other legal basis for the legality of processing (Article 17(1)(b) of the GDPR) and objections to data processing, as specified in Article 17(1)(c) of the GDPR, are additional mechanisms for restricting the use of personal data, which can also be included under the term "right to be forgotten". These mechanisms do not require any damage, which corresponds to the position of the CJEU. So, in the cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* the CJEU declared Directive 2006/24/EC invalid because it violated the principle of proportionality.[99] Taking into account the legal restrictions on data storage in this case, data protection once again becomes a collective right to protection rather than an individual one. Therefore, as U. Pagallo and M. Durante suggest, further rulings on the principles of data storage and the protection of both individual and collective rights in the "black box" society suggest that the right to erasure can also be considered as a key component of new forms of protection in the era of big data (for example, group privacy and collective data protection).[100]

Another justification for the right to be forgotten may be the concept of the right to personal identity. In this context, the right to be forgotten can expand its scope and gain a new dimension of essence. Information technologies have given a person the opportunity to project his/her identity in the digital space, which implies providing a person with those legal instruments with which he/she can do this, including through the right to be forgotten. Thus, P. Bernal and N. Andrade argue that the right to be forgotten can directly follow from the right to

---

[98] KÜHLING, Jürgen, RAAB, Johannes. Einführung, In KÜHLING, Jürgen, BUCHNER, Benedikt (eds.), *Datenschutz-Grundverordnung BDSG Kommentar*, 3rd edition, C.H. Beck, 2020, 26 p.; ALBRECHT, Jan Philip. *Die EU-Datenschutzgrundverordnung rettet die informationelle Selbstbestimmung!* Zeitschrift für Datenschutz, 2013, p. 587.

[99] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others*. 44 (2014), para. 69-71.

[100] PAGALLO, Ugo, DURANTE, Massimo. Human rights and the right to be forgotten. In SUSI, Mart (ed.) Human Rights, Digital Society and the Law: A Research Companion. 1st edition, *Routledge*, 2019, 412 p., p. 21

online identity.[101] This expansion of the right to be forgotten is due to a number of phenomenological changes, in particular with the appearance of a digital "self" that separates from the offline "self" and outlives the latter. The right to be forgotten as a mechanism for the formation and protection of human individuality can be seen as an expression of autonomy, through which each individual should be able to present and describe himself/herself on three levels: 1) the formation of personal identity through the revision of the past, 2) the connection between individual and collective memory and 3) various forms of oblivion in relation to the idea of forgiveness.[102] This understanding of the right to be forgotten makes it possible to apply it more widely as a right "to determine for themselves when, how, and to what extent information about them is communicated to others"[103] or as a right that gives an individual greater control over personal information. N. Tirosh argues that this right is not a guarantee of privacy, but rather the right to create their own narrative, appealing to the fact that people are given more "right of control" over their own personal data and, therefore, their identity.[104]

The recognition of a person's digital identity as a justification for the right to be forgotten corresponds to the case law of the CJEU, which reflects on the right to be forgotten as a certain emphasis on the assumption of the possibility of "managing" a digital person. In particular, in the judgment of the *Google Spain* case, a person is granted the right to withdraw a link from search engines. As one can see, this judgment gives a person a tool that allows him/her to control his/her digital identity. Thus, the right to be forgotten becomes one of the tools for the formation of digital identity and consideration of the right to be forgotten in this way may become a so-called paradigmatic shift in the issue of its justification of privacy, which will expand the scope of the right to be forgotten primarily through a departure from the balance with the right to expression or privacy for reasons of public interest, and they can only take place in exceptional circumstances, so the right to identity provides better protection than the right to privacy. In addition, such a justification can be deduced from the judicial practice of the ECtHR. In the case of *Tysiąc v Poland*, the ECtHR has confirmed that "private life" is a broad term covering, among other things, aspects of physical and social identity, including the right to personal

---

[101] See BERNAL, Paul A. The Right to Online Identity. SSRN Electronic Journal [online]. September 2012. [cit. on 25th December 2023]. Accessible at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143138>.; See also: ANDRADE, Norberto Nuno Gomes de. Oblivion: The Right to Be Different from Oneself - Reproposing the Right to Be Forgotten. *Revista de Internet, Derecho y Política*. No. 13, pp. 122-137.

102 PAGALLO, Ugo, DURANTE, Massimo. Human rights and the right to be forgotten. In SUSI, Mart (ed.) Human Rights, Digital Society and the Law: A Research Companion. 1st edition, Routledge, 2019, p. 21.

[103] Article 19. The Right to be Forgotten: Remembering Freedom of Expression. [online]. 2016. [cit. on. 25th December, 2023]. Accessible at: <https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf>.

[104] TIROSH, Noam. 'Reconsidering the "Right to Be Forgotten' – Memory Rights and the Right to Memory in the New Media Era. *Media, Culture & Society*, Vol. 39, No. 5, 2017, pp. 644–660.

autonomy, personal development, as well as to establish and develop relationships with other people and the outside world.[105] The right to be forgotten can become the right to represent an actual identity.

The case of *Google Spain* itself, which laid the foundations of the right to be forgotten in the EU's legal reality, caused a number of questions and uncertainties regarding the essence and nature of this right. As F. Ahmed notes: "(…) the ECJ has given rise to many questions regarding the implementation, applicability and effectiveness of the RTBF. There has been a significant change in the RTBF landscape and new issues have arisen which need to be sufficiently addressed in order to ensure proper implementation and application of the RTBF". [106] One of such obstacles is created by the judicial decisions of the European Supranational Courts themselves, which will be analysed in more detail and disclosed on the example of such cases as, for example, *GC and Others v. CNIL,*[107] *Khalili v. Switzerland,*[108] *M.L. and W.W. v. Germany*[109] and so on, which will be discussed further.

Thus, the right to be forgotten is a dynamic, multidimensional right that unites rights that have a different primary purpose, but have a common ultimate goal of protecting a person, his/her safety, honour, reputation, privacy, personal identity and dignity in the digital sphere from potential damage. The right to be forgotten in EU law, despite being a specification of the fundamental right to data protection, is nevertheless also an instrument of market regulation and redistribution of powers between data subjects and data processors, and has prerequisites for becoming a collective right. The right to be forgotten, which was originally born as the right to "forget one's criminal past", with the development of the Internet has the potential to become a broader right, with more opportunities and potential,[110] having acquired a different essence as a response to the modern challenges of the "Internet that never forgets".[111]

3.2 Theoretical Definition of the Right to be Forgotten

[105], ECtHR: Judgment of the Court of 24th September 2007, *Tysiąc v Poland*. No. 5410/03, para. 107.
[106] AHMED, Farhaan Uddin. Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm. *Computer and Telecommunications Law Review*, Vol. 21, No. 6, 2015, pp. 175-185.
[107] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 September 2019, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*. Case C-136/17.
[108] ECtHR: Judgment of the Court of 18th October 2011, *Khelili v Switzerland* (Application no. 16188/07).
[109] ECtHR: Judgment of the Court of 28th June 2018, Case of *M.L. and W.W. v. Germany* (Applications nos. 60798/10 and 65599/10)
[110] JONES, Meg Leta. Ctrl + Z: The right to be forgotten. New York: New York University Press. 2016, 75 p.
[111] CROCKETT, May. The Internet (Never) Forgets. *Science and technology Law Review*. 2017, Vol. 12, No. 2., pp. 151 – 181.

There is no unambiguous definition of the right to be forgotten. From a theoretical point of view, the definition of the right to be forgotten primarily encounters terminological diversity, which is used both in doctrine and in normative acts. Thus, the terms “right to be forgotten", “right to oblivion”, “right to erasure”, “right to deletion” and “right to de-list” are used. These terms are used as synonyms,[112] as elements of a particular right, or for the formulation of various concepts.

An analysis of the definitions of the right to be forgotten shows that it is primarily related to what kind of essence the determinant puts into it. There are two leading schools of thought that consider the different ontological scope of the right to be forgotten. The first school sees it as an extension of the right to deletion.[113] Thus, P. Bernal, distinguishing between the "right to be forgotten" and the "right to deletion", suggests that the latter, as a conceptual basis, is more consistent with how society should perceive personal data on the Internet today. According to the author, the "right to be forgotten" is, in fact, a version of the broader concept of the "right to deletion".[114] The latter is not related to giving individuals the opportunity to erase or change their personal history, but rather to giving them control over the data related to them, which shifts the focus from a specific act of erasure related to the right to be forgotten to data control. P. Bernal also considers the involvement of a third party as the second distinguishing factor between these rights. While the "right to be forgotten" involves delegating control to a third party, usually requested by the data subjects to delete their data, the “right to deletion” gives the data subjects the direct right to exercise control over their data.

The second school views it as an unfortunate misunderstanding and its supporters insist that the *Google Spain* case never established a “new” right, but simply clarified the scope of the right to deletion, while not taking into account the case law of the ECtHR.[115] De Terwangne concludes that the “right to deletion” and the “right to be forgotten” are synonymous,[116] and defines three different aspects of the “right to be forgotten”:

---

[112] BLANCHETTE, Jean-François, JOHNSON, Deborah G. Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness. *The Information Society*, Vol. 18, No. 1, 2002, pp. 33–45.
[113] KUNER, Christopher. The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges. In HESS, Burkhard, MARIOTTINI, Cristina M. (eds.). *Protecting Privacy in Private International and Procedural Law and by Data Protection: European and American Developments.* Baden-Baden: Nomos; Ashgate, 2015, pp. 19-55.
[114] BERNAL, Paul A.. A Right to Delete?. *European Journal of Law and Technology*, 2011, Vol. 2, No.2, pp. 1-18.
[115] HAMUĽÁK, Ondrej, et al. *The Global Reach of the Right to be Forgotten through the Lenses of the Court of Justice of the European Union.* Czech Yearbook of Public and Private International Law, 2021, Vol. 12, pp. 196-211.
[116] DE TERWANGNE, Cécile. The right to be forgotten and the Informational Autonomy in the Digital Environment. Publication office of the EU, 2013, Vol. 13, pp. 1-30.

1) *the concept of the right to oblivion of the judicial past*.[117]
2) *"the right to be forgotten, established by the legislation on data protection"*.[118] This aspect defines the right that gives data subjects the right to delete or anonymize their information after fulfilling the initial purpose of data collection.
3) *the right to be forgotten in relation to data that has expired.* This interpretation is often considered the broadest understanding of the "right to be forgotten", involving the application of an "expiration date" to data without the need for individual analysis.[119]

This classification, however, does not cover all possible situations, for example, in which individuals are granted the right to delete personal information posted by third parties, even if this information was accurate at the time of publication. *Google Spain* is an example of such a situation.

M. Jones and J. Ausloos argue that the right to be forgotten and the right to deletion (exclusion) of data are varieties of interpretation of the right to be forgotten.[120] Both concepts have different goals: while the right to be forgotten includes the concept of balancing conflicting interests to determine when a particular publication (information) is irrelevant to the general public, the right to deletion (exclusion) of data is more procedural in nature.[121]

J. Rosen identifies three categories of situations that fall under the right to be forgotten. The first category is related to the right of the data subject to control, in particular, the ability to delete information that he/she posted about himself/herself. This right is "acknowledged by the whole society as a right that [...] is effectively enforced through contractual provisions".[122] The second category refers to situations where a data subject publishes something and another person copies or reposts this content. Although J. Rosen does not conduct a detailed analysis of such data processing from the point of view of legality, however, the scholar assesses its compatibility with the GDPR. In particular, whenever an individual in such a scenario requests the deletion of their personal information from an Internet Service Provider (ISP), the ISP must immediately perform the deletion, unless data retention is considered "necessary" to protect

[117] Ibid., p. 11
[118] Ibid., p. 11
[119] Ibid., p. 11
[120] JONES, Meg Leta, AUSLOOS, Jef. The Right to Be Forgotten Across the Pond. *Journal of Information Policy*, Vol. 3, 2013, pp. 1-23.
[121] Access Now. Position paper: understanding the right to be forgotten globally. AccessNow. [online]. September 2016, [cit. on. 25th December 2023]. Accessible at: <https://www.accessnow.org/wp-content/uploads/2017/09/RTBF_Sep_2016.pdf>.
[122] STUPARIU, Ioana. Defining the right to be forgotten: A Comparative Analysis between the EU and the US. Budapest: Central European University. LL.M. Short Thesis. 2015, 84 p.

freedom of expression.[123] The third category includes situations where a third party publishes information about an individual (regardless of whether there is consent). J. Rosen points out that applying this expanded definition could have significant consequences, potentially turning search engines into "censors-in-chief for the European Union" rather than neutral platforms.[124]

B.J. Koops highlights two separate concepts of the right to be forgotten. The first one revolves around the human right to delete one's information within a reasonable time and includes a wider range of strategies that resemble the act of human forgetting.[125] This approach emphasizes the individual's control over his information and ownership of it. According to the second concept, known as a "blank slate", outdated negative information should not be used against people.[126] This view focuses on society as a whole, rather than on the rights of individuals.

It should be recognized that none of these definitions covers all the components of the right to be forgotten. It seems to us that when determining the right to be forgotten, it is necessary to focus on its multi-purpose essence and multidimensional content. It seems that the right to be forgotten is a collective term in relation to the above definitions. In our opinion, the right to be forgotten from the point of view of substantive law is a legal requirement that allows the erasure of "digital footprints" left on the Internet in order to protect the individual, his/her dignity, reputation, privacy and identity in the online world. Such a definition makes it possible to include both an individual and a possible collective requirement for such erasure.

A. Tamo and D. George point out that when deciding to accept the right to be forgotten, states should proceed from this broad definition, which they could adapt to their value system.[127] From the broad definition, one can also deduce a whole set of e-rights, each of which will have its own immediate separate purpose. The authors also argue that the right to be forgotten consists of "the substantial right of oblivion and the rather procedural right to erasure derived from data protection".[128]

Nevertheless, it seems that procedural rules cannot be included in the scope of the right to be forgotten. Although the current regulation specified in the GDPR gives grounds for such

---

[123] ROSEN, Jeffrey. The Web Means the End of Forgetting. New York Times Magazine. [online]. 21th July 2010. [cit. on. 25th December 2023]. Accessible at: <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all>

[124] Ibid.

[125] KOOPS, Bert-Jaap. Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to Be Forgotten" in the Big Data practice. *SCRIPTed.*, Vol. 8, No. 3, 2011., pp. 229-256.

[126] Ibid.

[127] TAMÒ, Aurelia, DAMIAN, George. Oblivion, Erasure and Forgetting in the Digital Age. *Journal of Intellectual Property. Information Technology and E-Commerce Law*. Vol. 71. No. 2, 2014, p. 74.

[128] Ibid.

an opinion. The simultaneous use of such a multitude of terms that are not only undefined, but also sometimes carry different semantic meanings, make the right in question uncertain, especially considering that there is no precise definition in normative acts or judicial practice.

3.3 Development of the right to be forgotten

3.3.1 Google Spain as a benchmark for the right to be forgotten

Elements of the right to be forgotten can be found in some legal acts even before *Google Spain*.[129] To grasp the pivotal importance of this decision, it is essential to understand that the Data Protection Directive (DPD) did not explicitly include the right to be forgotten. It offered a comprehensive definition of personal data and sensitive data, provided detailed definitions of processing, data controller, and data processor, regulated the right to data access, comprising several individual rights that formed the foundational basis for the right to be forgotten. It was primarily influenced by Convention 108, and this close connection was openly acknowledged in the Directive's recitals. These recitals stated that the principles of human rights and freedoms, especially the right to privacy, contained in the Directive, clarified and expanded upon the principles outlined in the Council of Europe's Convention from January 28, 1981 (Convention 108), which aimed to protect individuals in the context of automated processing of personal data.[130]

Over the decades since the adoption of the DPD, the volume of digitised content available online has increased exponentially. This evolution led to a greater interest from data subjects in protecting their rights within the online environment and their endeavours to exercise their right to be forgotten.[131] In 2011, a large number of complaints were sent to the Spanish State Data Protection Authority (AEPD) to remove links from the Google search engine, the publication of which is no longer in the public interest. The AEPD granted these complaints and ordered Google to take the necessary measures to remove personal data related

---

[129] In 1973, the recommendation to stop the rampant accumulation of data was enshrined in paragraph 21 of the Council of Europe resolution entitled "Protecting the privacy of individuals in relation to electronic data banks in the private sector." The German BDSG Law of 1977 defines the right to erasure and defines "confidential data". The right to erasure is also enshrined in paragraph of the 1980 OECD guidelines and in Article 8 of the Convention 108. With the adoption of the DPD in 1995, the right to erasure was directly legislated in EU law.

[130] See the Recital 11 of the DPD.

[131] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12,

to the applicants from its index and prevent access to such data in the future, thereby outlining the contours of the right to be forgotten, defending the protection of privacy.[132]

Among the complaints is also the complaint of Mr. Mario Costeja González. In 1998, the Spanish newspaper *La Vanguardia* published in its own print edition two ads about the forced sale of real estate of Mr. González in connection with his social security debt. These ads contained the name and surname of the citizen, and were subsequently published on the Internet. Mr. Costeja González appealed to the AEPD to *La Vanguardia* and *Google* with a demand to remove ads from the Internet, as well as links from search results, since the information contained in the ads is outdated - the forced sale of property was completed many years ago and he paid the requirements, therefore the public interest in disclosure of this information ceased to exist.

AEPD, considering González's complaint, on the one hand, confirmed the position of the Spanish edition of *La Vanguardia*, pointing out that the newspaper legitimately published ads on the forced sale of property ordered by the Ministry of Labor and Social Affairs of Spain, but on the other hand, the agency ruled that Google, acting as a data controller, should be responsible for the information available in the search engine. After such a decision, Google appealed to the Spanish High Court, which referred the case to the CJEU. The CJEU in the *Google Spain* case considered mainly the following questions:

1. If the European data protection framework established in the DPD is applicable to Google?
2. Is it possible to hold Google accountable as a data controller?[133] and
3. Is it possible to extend the right to deletion and the right to object to cover a request to delete data from an Internet search engine?[134]

The Court ruled that Google processed the personal data of Mario Costeja Gonzalez as a data controller. The Court, referring to the decision in the *Lindqvist* case, concluded that the activity of the Internet search engine as a content provider should be classified as "*processing of personal data*" within the meaning of Article 2(2) of the DPD.[135] By indexing data, Google extracts, records and organises data, even if Google indexing is performed automatically

---

[132] See CASTELLANO, Pere Simón. The Right to Be Forgotten under European Law: a Constitutional Debate. *Lex Electronica.* Vol. 16, No. 1 [online]. [cit. 2019-09-22]. Accessible at: <www.lex-electronica.org/docs/articles_300.pdf>.

[133] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12, para. 20.

[134] Ibid.

[135] Ibid, para.26.

without highlighting content. And the fact that the data has already been published on the Internet in the past and has not been changed in any way by the Internet search engine does not change this conclusion.[136] Accordingly, the Court considered Google as a data controller with the responsibilities that such a classification implies in accordance with the DPD.[137]

The most fundamental question is whether a data subject can require a search engine to remove the indexation of a certain piece of information.[138] The Court drew attention to Articles 12(b) and 14(a) of the DPD, which state that the data subject may require the data controller "erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data", as well as the provision on the right of the data subject to file an objection to data processing if he proves legitimate grounds related to a specific situation. If the data subject objects and he can successfully prove convincing legal grounds, the data controller must stop processing the personal data of the data subject, although the controller is not obliged to delete the already processed data.

The CJEU ruled that if the inclusion of certain links in search results at some point in time is incompatible with the provisions of the Directive, and the data subject requests this, such links must be deleted. The Court stressed that, in accordance with Article 7 of the Directive, data processing must be lawful at any time so that it can be continued.[139]

The CJEU stated that the processing may violate the fundamental right of the data subject to privacy and the right to personal data protection if such processing allows all Internet users to obtain a complete set of information about the data subject and search engines and create a detailed profile of the tracked person. In addition, even information originally collected in a legitimate way may become illegal to store over time when the data becomes inadequate, irrelevant or excessive for processing purposes.[140] In order for data processing to be incompatible with the Directive, the data does not have to be incorrect. It is sufficient that the data is inadequate, irrelevant or no longer relevant for data processing purposes or that it is stored longer than necessary for such purposes.[141]

The CJEU analysed the issue of the balance of private and public interests, recognizing that the "right to be forgotten" can be granted to a citizen only if there is no interest of the

[136] Ibid, para. 28.
[137] Ibid, para. 41.
[138] Ibid, para. 19-20.
[139] Ibid, para. 73.
[140] Ibid, para. 92-94.
[141] Ibid., See also Art. 6(c)- 6(e) of the DPD.

general public in access to information,[142] and also if the citizen does not represent a special public role.[143] The Court proceeded from the fact that in solving the problem of the correlation between freedom of expression (freedom of information) (Article 11 of the CFR) and the right to respect for private and family life (Article 7 of the CFR), the right to personal data protection (Article 8 of the CFR), the latter two rights (Articles 7-8 of the CFR) outweigh in this case.[144]

So, based on Directive 95/46, the CJEU in paragraph 72 of its judgment determined that links to data about a citizen can be removed by the controller from the search results if:

1. the data about the subject is incompatible with the original purposes and rules of personal data processing, and was obtained illegally by the controller;
2. information about the person is unreliable and irrelevant;
3. information about the subject is irrelevant or excessively redundant.[145]

According to the Court, it is precisely such criteria in relation to personal data that determine the possibility of a citizen exercising the "right to be forgotten".[146] So, in the *Google Spain* case, the CJEU interpreted the DPD as creating a presumption that Google should remove links to personal information from search results at the request of the data subject, unless a strong public interest suggests otherwise.

3.3.2 Criticism of *Google Spain* judgment in the doctrine

The *Google Spain* case has been the subject of debate and criticism. In the conclusion of this case, AG N. Jääskinen supported Google's position, pointing out that the Google search engine is not obliged to remove links from the search engine, since the information is publicly available, and the removal of such information restricts freedom of expression and violates the principles of objectivity of information. In his opinion, Article 12(b) and Article 14(a) of the DPD are not equivalent to the right to be forgotten, such a right is nowhere contained in the

[142] Ibid, para. 97-99.
[143] Ibid.
[144] LYNSKEY, Orla. Rising like a Phoenix: The «Right to be Forgotten» before the ECJ. THE EUROPEANBLOG [Online]. 13th May 2014. [cit on. 25th December 2023]. Accessible at: <http://europeanlawblog.eu/2014/05/13/rising-like-a-phoenix-the-right-to-be-forgotten-before-the-ecj/>
[145] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12, para. 72.
[146] OWINGS, Lisa. The Right To Be Forgotten. *Akron Intellectual Property Journal*. Vol. 9, No. 1, 2015. pp. 45-82.

current EU legal framework for cases in which the publication of information is *de facto* legal.[147]

AG N. Jääskinen pointed out that the application of Article 14(1)(b) of the DPD requires an objective assessment of the purpose of processing and the interest in processing personal data, on the one hand, and the legitimate interests of the data subject, on the other hand. In these circumstances, the right to object could only be exercised if the Internet search service provider went beyond its intermediary functions and assumed responsibility for the content provided on the source website. The AG argued that granting the right to be forgotten could not be justified, because it would lead to the sacrifice of fundamental rights such as freedom of expression and the right to information. According to the AG, such an approach can lead to the automatic removal of links to any questionable content or an unmanageable number of requests that would have to be processed by the most popular and important Internet search engine service providers.[148]

The researchers in the field of information law also criticised the judgment under consideration. For some, this has become an example of the ever-growing imperialism of EU data in the field of regulation.[149] Others even considered that such a right could not exist. Thus, E. Peucker believes that the right to be forgotten is just a fancy word, but not an established legal concept, considering lawyers' attempts to use this terminology as an "obsession".[150] R. Posner believes that the right to privacy in the context of the "right to be forgotten" is a form of selfish economic behaviour, since it allows to conceal certain facts for one's own benefit.[151] The criticism is also justified by the fact that very little information is available to the public about the type and number of links that are removed from search results, the number of deletion requests, the number of rejected requests and so on.

Many criticised the decision for giving too much authority to private organisations to censor the Internet without providing sufficient guidance on implementation. Moreover, requests are being considered or decisions are being made on them "entirely inside a private

---

[147] Opinion of Advocate General Jääskinen delivered on 25 June 2013, Case C-131/12, para. 111.
[148] Ibid, para. 133.
[149] BOWCOTT, Owen. "Right to be forgotten" could threaten global free speech, say NGOs'. The Guardian [Online]. 9th September 2018. [cit. on. 25 December 2023]. Accessible at: <https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos>.
[150] PEUCKER, Enrico. The "right to be forgotten" in Germany. In: TAMBU, Olivia (ed.). *The right to be forgotten in Europe and beyond/ The right to love in Europe and beyond*. 2018, Luxembourg: Blogdroiteuropéen, Open access collection, 34-40 p.
[151] POSNER, Richard A. Economic Analysis of Law, Economic Analysis of Law, 5th edition, *Aspen*, Vol. 46, 660-663 pp.

corporation, without public accountability or scrutiny".[152] As a result, "Google found itself both judge and jury regarding the relevance of requests for de-referencing". [153]

The next line of critical arguments is that the court incorrectly recognized Google as a data controller subject to the Directive, and that the judicial balance test ignored basic legal principles and rights. The Court interpreted the term "data controller" excessively broadly, including search engine operators. R.T. Nurullaev indicates that: "the court's decision to classify search engine operators as controllers with respect to processing of indexed personal data is problematic for at least two reasons".[154] "Firstly, search engine operators in practice cannot comply with all the obligations imposed on data controllers" due to the difficulties of obtaining consent to the processing of personal data by search engine operators, as well as due to the technical features of the search engine operation. [155] Secondly, a fairly broad interpretation of the concept of "data processing" creates problems in practice when defining a particular entity as a data controller. Thus, R.T. Nurullaev gives an example of the fact that Internet users can also be identified as data controllers, since they (users) search for information in a search engine and thereby extract personal data about a subject from an array of information.[156]

It was also criticised that the CJEU put the right to privacy above the right to freedom of expression, although there is no hierarchical relationship between conflicting human rights.[157] However, it should be pointed out that the latter fact can be justified by the desire to ensure the protection of the individual, giving the latter the authority to control the use of his/her personal data. A.S. Sweet noted that the Court used the situation in its efforts to improve the effectiveness of EU legislation.[158]

O. Gstrein notes that there are three questions that were remained without response in the judgment of the Google Spain case, in particular: 1) the lack of direct legal supervision and

---

[152] O'BRIEN, Danny, YORK, Jillian. Rights that Are Being Forgotten: Google, the ECJ, and Free Expression, Electronic Frontier Found [online]. 8th July 2014, [cit. on 23th December 2023]. Accessible at: <https://www.eff.org/deeplinks/2014/07/rights-are-being-forgotten-google-ecj-and-free-expression>.

[153] KUCZERAWY, Aleksandra, AUSLOOS, Jef. From notice-and-takedown to notice-and-delist: Implementing Google Spain. *Colorado Technology Law Journal*, 2016, Vol. 14, No. 2, pp. 219-258.

[154] NURULLAEV, Ruslan. Right to Be Forgotten in the European Union and Russia: Comparison and Criticism. *Pravo. Zhurnal Vysshey shkoly ekonomiki.* 2015. No. 3. P. 181-193.

[155] Ibid.

[156] Ibid.

[157] HUSOVEC, Martin. Should We Centralize the Right to Be Forgotten Clearing House? Center for Internet and Society [online]. 30th May 2014, [cit. on. 25th December 2023]. Accessible at: <https://cyberlaw.stanford.edu/blog/2014/05/should-we-centralize-right-be-forgotten-clearing-house>.

[158] STONE SWEET, Alec. The European Court of Justice and the judicialization of EU governance. *Living Reviews in European Governance.* 2010, p. 1. See Also: DE HERT, Paul, PAPAKONSTANTINOU, Vagelis. 'Google Spain: Addressing Critiques and Misunderstandings One Year Later'. *Maastricht Journal of European and Comparative Law*, Vol. 22, No. 4, 2015, pp. 624–638.

transparency for the procedure of removal of personal information; 2) the content publisher's right to be heard and 3) the territorial scope of the application.[159]

At the same time, when analysing the issue of fundamental rights, the CJEU refers only to its own case law and ignores the judgments of other jurisdictions. The Court ignored references to ECHR and the case-law of ECtHR, which creates the risk that the same rules of law will be interpreted differently by different jurisdictions.

Obviously, the ruling in the *Google Spain* case is not without flaws. First of all, the significance of this judgment in determining the right to be forgotten seems to me to be somewhat exaggerated, because it was made according to the procedure of Article 267 of the TFEU and was binding only "*inter partes*" and did not create a precedent in accordance with the "*stare decisis*".

In addition, the CJEU has practically delegated the definition of the contours of the right to be forgotten to search engines. Thus, private organizations have become a kind of legislator for the right to be forgotten, as I have previously indicated. Given the lack of transparency of information about request processing, this will make the application of the right to be forgotten problematic.

The Court also failed to clarify the cases and circumstances in which the prevailing public interest would require constant access to information and when instead the information is no longer relevant.[160] The Court explained that the balance between the right to be forgotten and the public interested in the disputed information requires an individual assessment, but without determining what criteria and procedures are necessary for this.

The CJEU in its *Google Spain* judgment used terms such as "*inadequate*", "*irrelevant*" and "*excessive*" to indicate the moment when the purpose of data processing was achieved. The purpose limitation is a key principle of data processing in the EU. For example, data related to convictions and offenses cannot be processed without consent or special authority. However, there are legitimate reasons to continue processing data even after the initial purpose has been achieved, for example, in journalistic activities. But what happens to data that can never be processed due to inappropriate disclosure of the identity of witnesses or fails to reach the purpose due to public interest? Or even if the purpose is achieved, but the data is needed for

[159] GSTREIN, Oskar J. The Judgment That Will Be Forgotten'. Verfassungsblog: On Matters Constitutional [online]. 25th September 2019. [cit. on. 25th December 2023]. Accessible at: <https://verfassungsblog.de/the-judgment-that-will-be-forgotten/>.

[160] FORDE, Aidan. Implications of the Right To Be Forgotten. *Tulane Journal of Technology and Intellectual Property*. 2015, Vol. 18., p. 107.

public interest? There are ambiguities here, since there is no clear time frame for determining when the data processing purpose is achieved.

Unfortunately, the uncertainties in interpretation were not eliminated in Article 17 of the GDPR. In this context some scholars have critically perceived the emergence of the phenomenon of the right to be forgotten in the European legal reality, considering it as "unforgettable fiasco, (...) morphing into a nightmare for the web giant",[161] "an emerging threat to media freedom in the digital age",[162] "that threatens to censor entire swathes of the web". [163] As E. Lee notes: "The EU right to be forgotten is a new privacy right (or a new application of privacy to Internet search engines) that has sparked great controversy around the world. The major concern among critics of the judgment is that it will lead to censorship of information on the Internet by making it difficult, if not impossible, to find relevant articles associated with a person."[164] The same position is held by E. Politou, A. Michota and others, claiming that: "the RtbF caused prolonged controversies due to its pivotal impact on current data processing procedures and its unavoidable conflicts with other rights such as the right to free speech and the freedom of information, especially in the era of big data and the Internet of Things (IoT)".[165]

3.3.3 The right to be forgotten after the *Google Spain* case

A. The GDPR

The judgment of the *Google Spain* case, as well as the very consideration of the issue in the CJEU had some influence on the development of the text of Article 17 of the GDPR, but such an impact was too insignificant. Thus, when Google Spain was accepted for consideration, the title of Article 17 was changed from "the right to erasure" to "the right to be forgotten". [166]

---

[161] WOHLSEN, Marcus. For Google, the 'Right to Be Forgotten' Is an Unforgettable Fiasco. WIRED [online]. 3th July 2014. [cit. on. 25th December 2023]. Accessible at: <https://www.wired.com/2014/07/google-right-to-be-forgotten-censorship-is-an-unforgettable-fiasco/>.

[162] OGHIA, Michael J. Information Not Found: The "Right to Be Forgotten" as an Emerging Threat to Media Freedom in the Digital Age. CIMA Digital Report [online]. 9th January 9 2018. [cit. on. 25th December 2023]. Accessible at: <https://www.cima.ned.org/publication/right-to-be-forgotten-threat-press-freedom-digital-age/>.

[163] SOLON, Olivia. EU 'Right To Be Forgotten' Ruling Paves Way for Censorship. WIRED [online]. 13th May 2014 [cit. on. 25th December, 2023]. Accessible at: <http://www.wired.co.uk/news/archive/2014-05/13/right-to-be-forgotten-blog>.

[164] LEE, Edward. The Right to Be Forgotten v. Free Speech. *A Journal of Law and Policy for the Information Society.* Vol. 12, No. 1. 2015, p.110.

[165] POLITOU, Eugenia, et. at.: Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*. 2018, Vol. 34., No. 6., pp. 1247-1257.

[166] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' (European Parliament, 12 March 2014) accessed 24 October 2019.

After *Google Spain*, the wording of the right to be forgotten "returned" to the title of Article 17 of the GDPR, but the very essence of the article has not changed. The change did not address important factors for the exercise of this right, for example, questions about whether search results should also change for non-European domains and whether media websites should also delete articles after a certain period of time remain open.

Article 17 of the GDPR did not actually create a separate new right to be forgotten, but concentrated on clarifying and formalising the process of deleting personal information defined in the DPD to exercise the right to erasure. Meanwhile, the CJEU did not consider the right to be forgotten as identical to the right to erasure. It is also worth noting that the specific right to be forgotten created by the *Google Spain* judgment is not directly established in the GDPR. Some of its aspects are indirectly reflected in Article 17(2), which requires the data controller to inform other controllers about the data subject's request to delete links, copies or replications of personal data.

According to Article 17(1) of the GDPR, the data controller is obliged to immediately delete personal data at the request of the data subject in several cases: 1) if the subject has withdrawn his/her consent or objected to the processing of data, 2) if this data is no longer needed for the purposes for which it was collected, or 3) if the data processing is carried out illegally. This "classic" right to deletion of data can be used against any data controller, that is, a person or organization that determines the purposes and methods of data processing. It is based on the proprietary concept of privacy and provides the data subject with the opportunity to withdraw their consent to the use of their data, issued to the data controller. The scope of the provisions of Article 17 of the GDPR is much broader than the rights set out by the CJEU in the *Google Spain* case: it is not limited to search engines, covers all personal information and provides protection not only in cases of loss of interest in past irrelevant information, but also in other situations such as illegal processing or withdrawal of consent.[167]

Nevertheless, in the absence of any legislatively fixed scope of the right to be forgotten and criteria for balancing it with other rights, the Court began to form the scope of this right through its law enforcement practice.

B. The case-law of the CJEU

As it is known, the CJEU plays an important role in the issue of personal data protection, since its function is to interpret EU legislation and, consequently, EU legislation related to the

[167] OVČAK KOS, Maja. The right to be forgotten and the media. *Lexonomica.* Vol. 11, No. 2, 2019, pp. 195–212.

protection of personal data.[168] The CJEU through its judicial practice has contributed to the transformation of personal data protection into a fundamental right by defining the categorical apparatus used in relevant legal acts, obligations and responsibilities of the parties involved in data processing, balancing data protection with other rights.[169] Due to the uncertainty of the regulation of the right to be forgotten in the EU legislation itself, the role of judicial practice is especially important because it is an attempt to develop guidelines for the correct application of this right.

It is necessary to emphasise the rethinking of the role of the CJEU itself in the field of the right to be forgotten. The formation of the right to be forgotten in the context of the EU case law, especially when it is associated with the problem of the conflict of the right to privacy with the right to information and freedom of expression and with the development of difficult-to-predict technology development, can certainly be considered the best option for including the right to be forgotten in the EU legal order. In this case, not regulating the right to be forgotten in the form of any legal act and leaving its regulation solely at the discretion of the judicial practice of the CJEU can create a flexible legal framework for the right to be forgotten. However, the Court's interpretation of EU law is limited by the exhaustive list of cases in which it can make decisions (preliminary rulings, etc.) referred to in Article 10(1) of the TFEU. In addition, the CJEU has indicated in its practice that the binding nature of its judicial decision on the interpretation of EU law cannot be understood in terms of *res judicata*, since this is not a final judicial decision, but only a preliminary ruling.[170]

The *Google Spain* case concerned the provisions of the DPD, a legal document whose purpose, according to Article 1(1), is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. And therefore, it is in the order of things that the CJEU assessed the possibility of applying the right in question in the context of this purpose.

---

[168] PAVELEK, Ondřej, ZAJÍČKOVÁ, Drahomira. Personal Data Protection in the Decision-Making of the CJEU Before and After the Lisbon Treaty. *Baltic Journal of European Studies*. 2021, Vol. 11, No. 2, p. 167.

[169] Judgment of the Court (Grand Chamber) of 6 October 2015, *Maximillian Schrems v. Data Protec-tion Commissioner*, Case C-362/14 EU:C:2015:650; Judgment of the Court (Second Chamber) of 9 March 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, Case C-398/15; EU:C:2017:197, Judgment of the Court (Grand Chamber) of 5 June 2018 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*. Case C-210/16. EU:C:2018:388; Judgment of the Court of 6 November 2003, *Criminal proceedings against Bodil Lindqvist*, Case C-101/01.EU:C:2003:596; Judgment of the Court (Second Chamber) of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14 EU:C:2016:779 and so on.

[170] See, for example, Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 October 2018, *Hessische Knappschaft v. Maison Singer and sons*, Case C-234/17.

Subsequent judicial practice of the CJEU does not form a common vision and accuracy in the development and implementation of the legal framework of the right to be forgotten, however, it forms the scope of the right to be forgotten case-to-case. Thus, already in the *Manni* judgment, the Court found that the public interest in preserving data in state registers is so strong that the right to be forgotten is excluded here. The Court considered, on the one hand, the EU's data protection rights and Mr. Manni's commercial interest in deleting information about the bankruptcy of his former company, and, on the other hand, the public interest in accessing information. The Court recalled the fact that such publication of information in the public register of companies is enshrined in law for the implementation of the EU Directive. The Court ruled that Mr. Manni had no right to request the deletion of his personal data, since his rights under the applicable data protection law were overturned by the need to protect the interests of third parties in relation to public limited liability companies and limited liability companies to ensure legal certainty, fairness of commercial transactions and, consequently, proper functioning of the domestic market. Thus, such disclosure does not lead to disproportionate interference with the fundamental rights of the persons concerned and, in particular, with the rights guaranteed by Articles 7 and 8 of the CFR.[171]

The CJEU continued the established judicial practice with the *Google Spain* case. In 2022, the CJEU ruled on the case of *TU and RE v Google LLC*.[172] The case concerned the interpretation of Article 17(3)(a) of the GDPR, Article 12(b) and Article 14(1)(a) of the DPD. On the one hand, the court clarifies the interpretation of Article 17 of the GDPR, expanding the scope of the right by including photographs and "miniatures" in the right to "de-reference the links" and, on the other hand, defines the operator's obligation to conduct a separate assessment of search engine results. The CJEU had to answer two questions in this case:[173]

How should the courts consider requests to exclude links in cases where applicants claim that the information provided by a news outlet is inaccurate, and when the legality of the publication depends on whether these statements correspond to factual reality?

Are search engine providers such as Google required to remove thumbnails from search engine results, even if the results contain a link to the original source?

In its judgment, the Court reiterated that the processing of information by search engine providers should be considered regardless of the initial publication of the content, which is

[171] Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 9 March 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, Case C-398/15, para. 57.
[172] Judgment of the Court (Grand Chamber) of 8 December 2022. *TU and RE v Google LLC.* Case C-460/20.
[173] Ibid, para. 39.

consistent with the *Google Spain* decision and subsequent judicial practice.[174] The Court then focuses on Article 17(3)(a) and repeats that any restriction on the right to be forgotten must be provided for by law, respect the essence of the rights, be necessary, proportionate and truly meet the purposes of the common interest recognized by the EU.[175] Although in the judgment in the case *GC and Others*,[176] the Court has slightly changed its approach to this issue, however, in the judgment of the case *TU, RE v. Google*, the Court repeats the statement that, as a rule, the rights of data subjects to protect their privacy and data outweigh the interest in access to information.[177] In deciding whether links to thumbnails in search engine results should be removed within the legal framework of the DPD, the CJEU applies a similar approach: search engine operators should conduct an assessment when it comes to the use of thumbnails and images, taking into account the added value of public discussion and taking into account that the protection of personal information prevail by default. Search engine operators should conduct an independent assessment, weighing the value of the images for public discussion and taking into account any text accompanying the images.

In addition, the CJEU considers that the search engine operator cannot be required to actively verify the information provided by the applicant.[178] But at the same time declares that if the person seeking the removal of the links represents "relevant and sufficient evidence capable of substantiating his or her request and of establishing the manifest inaccuracy of the information".[179] The search engine operator is obliged to remove the link to the relevant content. In cases where the presented evidence of unreliability of information is not obvious, search engine operators are not required to remove links to the results without a judicial decision.

The judgment also strengthens Google's obligation to verify and provide accurate information. The strengthening of this obligation can be observed in both DSA and DMA. It is possible to consider the emergence of such a duty in the context of the transition from a libertarian understanding of cyberspace[180] to an understanding of multi-stakeholder Internet governance.[181] In this case, the search engine operator must conduct a separate assessment that

---

[174] Ibid, para. 50.
[175] Ibid, para 57 and further.
[176] Judgment of the Court (Grand Chamber) of 24 September 2019, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL),* C-136/17.
[177] Ibid, para. 62.
[178] Ibid, para.70
[179] Ibid, para 72
[180] BARLOW, John Perry. A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation [online]. 8th February 1996. [cit. on. 25th December 2023]. Accessible at: <https://www.eff.org/cyberspace-independence>.
[181] HILL, Richard. Internet Governance, Multi-Stakeholder Models, and the IANA Transition: Shining Example or Dark Side? *Journal of Cyber Policy*, Vol. 1, No. 2, 2016, pp. 176-197.

follows the principles established to ensure a balance of fundamental rights such as privacy and data protection, freedom of expression, freedom of doing business, as well as public interest in access to information and diversity of opinions.

So, the consistent practice of the CJEU confirms the right to be forgotten in the EU legal order, expanding the scope of its application. Although the judgments of the CJEU can be seen as a logical and consistent step in expanding the CJEU's case law on this issue after the case of *Google Spain*, nevertheless, the right to be forgotten in the EU and beyond also highlights the lack of a common vision of the right in question. The lack of a suitable regulatory framework for defining its contours cannot be considered correct. The case law of the CJEU will be discussed in more detail in the following chapters.

4 The scope of application of the right to be forgotten in practice

4.1 Territorial scope of the right to be forgotten

The territorial scope of application of legal frameworks in the digital world is the subject of much debate. The difficulties of regulation are primarily related to the boundlessness of information flows and the enormity of data processing technologies.

With the adoption of the GDPR, the issue of territorial coverage has become even more acute due to the rather broad definition in Article 3 of the GDPR. First of all, this has the purpose of preventing circumvention of the law, which would leave data subjects unprotected.[182] A clear definition of the scope of the GDPR is important to ensure the effective regulation of the relevant legal relations, and in the context of this dissertation, such a definition should be crucial for the applicability of the right to be forgotten. Article 3 of the GDPR divides the territorial coverage into three situations:

1) The EU establishment-criterion (Art. 3(1) of the GDPR);
2) The EU targeting-criterion (Art. 3(2) of the GDPR); and
3) Applicability by virtue of public international law (Art. 3(3) of the GDPR)[183].

In following section, I will consider the above situations in more detail.

4.1.1 The EU establishment-criterion (Art. 3(1) GDPR)

Article 3(1) establishes a default rule for determining the territorial applicability of the GDPR. According to the article 3(1) of the GDPR, it is applied when data processing operations take place in the context of the activities of an establishment, either a controller or a processor in the EU. In a simplified way, the following situations can be envisaged:

a) the data subject, data controller/processor and establishment are located within the EU;
b) the data controller/processor is located outside the EU;

---

[182] Recital 23 GDPR. Also see: Article 29 Working Party, Opinion 8/2010 on Applicable Law, 2010, WP 179 28 [online]. Accessible at: <http://ec.europa.eu/justice/article-29/documentation>; SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation. *International Data Privacy Law*. Vol. 5, No. 4, 2015, pp. 226-234.

[183] The third set of situations is when an international treaty or custom dictates the applicability of EU law. Its practical significance in the context of this thesis is insignificant and therefore will not be discussed.

c) the data subject is located outside the EU;

d) the establishment is located within the EU.

The situation specified in paragraph (a) clearly falls within the territorial scope of the GDPR. For other situations mentioned above, the use of the GDPR is problematic. The GDPR does not provide a definition of '*establishment*' but the Recital 225 clarifies that an *"establishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect"*. It is identical to what is indicated in Recital 19 of the Directive 95/46/EC, which has been referred to in several CJEU rulings. In the *Google Spain* case, the CJEU found that the US-registered company Google Inc. was subject to EU law, because its search activity was sufficiently linked to the advertising sales provided by Google's local subsidiary in Spain. Since the data processing in question in this case was related to a search business that helped finance the sale of online advertising to *Google Spain*, the CJEU found that the processing was carried out "*in the context of the activities*" of a Spanish establishment. The CJEU defends the flexible definition of "*establishment*". So in the *Weltimmo* case,[184] the CJEU indicates that the concept of establishment must be interpreted broadly. The legal form of such establishment (e.g. branch, subsidiary etc) is not the determining factor. The formalist approach whereby organizations are considered to be established solely in the place in which they are registered is not the correct approach. There is a test: (i) Is there an exercise of real and effective activity — even a minimal one? (ii) Is the activity through stable arrangements? and (iii) Is personal data processed in the context of the activity?

The inclusion of the words *"in the context of activities"* clearly underlines the intention of the legislator to define a broad (territorial) scope of application. This terminology implies that the EU establishment itself is not obliged to actually process personal data or to be directly involved in the processing of personal data. The CJEU pointed out that the simple availability of the service in a member State is not enough.[185] In the *Google Spain* case, the CJEU explained that it is sufficient that the activities of an institution in the EU are inextricably linked to the data processing activities of a controller/processor outside the EU. This criterion is "*inextricably linked*" and confirms the functional approach to interpreting the territorial scope

[184] Judgment of the Court (Third Chamber) of 1 October 2015, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*. Request for a preliminary ruling Case C-230/14.

[185] Judgment of the Court (Third Chamber) of 28 July 2016. *Verein für Konsumenteninformation v Amazon EU Sàrl*. - Case C-191/15., para. 76.

of data protection. Similarly, WP29 emphasizes the importance of taking into account the degree of involvement of an establishment, the nature of its activities and the purpose of the data protection laws, which is to effectively protect.[186] In conclusion, it should be noted that the question of whether processing activities are carried out in the context of the establishment's activities in the EU should be decided on a case-by-case basis.

So, Article 3(1) of the GDPR establishes the definition of the territorial scope of the EU data protection law by default. It indicates that the determining factor is the context in which the processing is carried out, and not where the personal data is physically located and/or processed.[187] This functional interpretation has been confirmed by both WP29 and CJEU. Data controllers and processors have obligations under the GDPR whenever processing is carried out "*in the context of the activities*" of the relevant establishments, regardless of whether it is carried out by the *"relevant establishment"* or not. The determination of whether processing is carried out *"in the context of the activities"* is made on a case-by-case basis, taking into account specific facts and in the light of relevant judicial practice.

The situation in paragraph (b) concerns a controller (processor) located outside the EU, while both the data subject and the establishment (controller/processor) are located within the EU. In such circumstances, the issue of whether personal data is being processed "*in the context of the activities of an establishment in the Union*" will be considered.

The last two scenarios rather atypically relate to situations where the data subject – a person potentially enjoying the right to erasure – is located outside the EU. The GDPR does not discriminate between EU citizens and non-EU citizens and theoretically, anyone outside the EU can invoke the rights of a data subject in accordance with the GDPR. The key point in assessing territorial applicability in these situations will be whether the actual processing actions that are being challenged occur "in the context of the activities of the (establishment) controller/processor within the EU". The more organisations involved in processing are located outside the EU (potentially controller(s), processor(s) and/or data subject), the more difficult it will be to declare the application of GDPR by virtue of Article 3(1) of the GDPR.

4.1.2 Targeting data subjects in the EU

[186] Article 29 Working Party, Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgment in Google Spain, p. 15.

[187] Not in the least to prevent circumvention by mere relocation of the controller/processor's corporate seat for example. See also Ibid. p. 16.

Article 3(2) of the GDPR defines the situations in which the GDPR can be applied, even if the controller/processor does not have representation within the EU. This article guarantees that data subjects in the EU can invoke their right to erasure in relation to non-EU organisations that target them in one way or another, i.e.: a) offering of goods or services to such data subjects in the EU; or b) monitoring of their behaviour as far as their behaviour takes place within the EU.

In fact, the idea of focusing on "targeting individuals" has been used in many European legal systems.[188] At the end of 2015, WP29 reaffirmed its defence of such a "principle of consequences", complementing the principle of territoriality.[189] In general, the provision is definitely consistent with the justification of the fundamental right to data protection. The interpretation of the (territorial) scope of application of the right should be carried out in the light of effective and complete protection of data subjects.

In the case of offering goods and services, controllers and processors established outside the EU are subject to the GDPR when they process personal data in relation to goods or services offered to data subjects within the EU. This means that the right to erasure can still be applied to non-EU-based controllers. Determining whether the controller/processor actually offers goods/services to data subjects in the EU requires a functional approach, taking into account the specific circumstances of each individual case. In light of this, the GDPR states that simply accessing their website and/or contact details from the EU will not be enough.[190]

The GDPR also applies to controllers/processors established outside the EU when they monitor the behaviour of data subjects within the EU. This means that data subjects can invoke their right to be forgotten in relation to a foreign controller who monitors their behaviour when surfing the web. It is important to note that Article 3(2) of the GDPR covers only the behaviour of the data subject occurring in the EU.[191]

---

[188] WP29 refers specifically to Article 15(1)(c) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 12, 16.1.2001, p.1), interpreted by Advocate General Trstenjak in 18 May 2010, in the case of C- 144/09, *Hotel Alpenhof*. The WP29 also cites US legislation on the protection of Children: COPPA, 16 CFR 312.2, [online]. Accessible at <http://www.ftc.gov/os/1999/10/64fr59888.pdf>, p. 59912. More examples are given in: KORFF, Douwe. New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments. *European Commission DG Justice, Freedom and Security Report,* 2010 [online]. Accessible at: <https://ssrn.com/abstract=1638949>.

[189] Article 29 Working Party, 'Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgment in Google Spain' (n 691), pp. 5–6

[190] See in this regard also Judgment of the Court (Third Chamber) of 28 July 2016. *Verein für Konsumenteninformation v Amazon EU Sàrl.* - Case C-191/15., para. 76.

[191] Originally, the provision did not specify the behaviour itself had to take place within the EU. As a result, an EU citizen's shopping behaviour in an Australian clothing store, for example, would also be captured by the GDPR's extra-territorial reach. See also: SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU

Article 3(2) of the GDPR significantly expands the extraterritorial scope of the GDPR. The GDPR mitigates the consequences of its extraterritorial spread from the point of view of law enforcement. Article 27 of the GDPR, for example, requires the appointment of a representative to the EU whenever Article 3(2) of the GDPR applies.

The targeting provision has been criticised. So, D. Svantensson argues, that "for a large number of parties involved in the handling of personal data, courts are going to have to conclude either that they target just about every country in the world or no countries at all".[192] He describes the "targeting approach" quite sharply as "the legislator's (and some academics') dream, but the judge's (and indeed lawyer's) nightmare".[193] This situation also undermines the legitimacy of the GDPR.[194] Thus, the right to erasure can be used against ISS providers that do not have a representative office in the EU, if they target people (data subjects) in the EU or simply monitor their behaviour.

4.2 Material scope of the right to be forgotten

Article 2 of the GDPR defines the material scope of the GDPR. In order to accurately determine the application of GDPR, it is especially important to determine what *a) personal data* and *b) processing* are.

4.2.1 Defining personal data

The EU data protection system is a legislative act focused on personal data, therefore, the definition of personal data determines the subject of most of the rights of data subjects, especially the right to be forgotten. Without understanding what personal data is, it is impossible to determine which data can be erased or "forgotten". In accordance with Article 4(1) of the GDPR "personal data" means:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an*

---

data privacy law: The weak spot undermining the regulation. *International Data Privacy Law*. Vol. 5, No. 4, 2015, p 230.

[192] Ibid.

[193] Ibid.

[194] Article 29 Working Party, Opinion 8/2010 on Applicable Law, p. 17.

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

WP29 breaks this definition down into four elements:

A. *information;*
B. *related to;*
C. *identified or identifiable;*
D. *to an individual (natural person).*

Many researchers criticise the legislative concept of personal data because of its unreasonable breadth. So, P. Schwartz and D. Solove suggest that absolute and irreversible anonymity is no longer possible today and suggest to save personal data as a protection threshold, but with a clearer definition, namely based on the risk of identification with "0". (zero risk of identification) to "*identified*" and treat information with varying degrees of identifiability differently. [195] The concepts of *"identified"* and *"information relating to"* require an interpretation of what constitutes an appropriate identification opportunity and an appropriate relationship between information and an individual (natural person).

A. "Any information"

According to WP29, any information may fall under the concept of "*personal data*" regardless of its nature, content or format. It may represent personal data regardless of the medium or form that may be "*alphabetical, numerical, graphical, photographical, or acoustic*"[196] subject to other criteria for determination. The information does not necessarily have to relate to private or family life and may relate to a person's life, his/her professional and other qualities.[197]

WP29 refers to "*information*" as a concept whose meaning is obvious. But the concept of information has different meanings, and adopting such a broad approach to information leaves the concept of personal data wide open for potential application and interpretation,

[195] SCHWARTZ, Paul M., SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 2011, Vol. 86, p. 1814.
[196] Article 29 Working Party, Opinion 8/2010 on Applicable Law, p. 17.
[197] Ibid.

subject to other conditions. The result may be information or contain information that may be personal data, subject to other requirements of the definition.

The meaning of the term "*any information*" was first considered in the *Nowak* case. The CJEU has ruled that this term reflects the purpose of the EU legislature "to assign a wide scope [concepts of personal data] to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments".[198]

This interpretation corresponds to the broad approach of WP136, according to which any information can be personal data, regardless of its nature or content. However, the Court also did not define what information is.

The GDPR treats data and information as synonymous, yet in theory disputes are based on a conceptually clear distinction between the form of information and the information itself.[199] But this clear distinction is not supported by the GDPR, on the contrary - by using synonymy of data and information, it allows the possibility of protecting both the form of information and the information itself.

But the characteristics of the data depend on the nature of the information: if the information contained in the data is personal, then the data is personal. This circumstance focuses attention to the position that: "(...)EU law defines personal data reversely: data are the source of information which, if personal, reversely implies that the original data are also personal. This definition leads into a seemingly paradoxical situation in which no data are personal from the outset and all data can become personal from the outset".[200] Synonymous data/information may be included in the definition of Article 4 of the GDPR, in order to extend the material scope of the GDPR protection, to include protection and information that, regardless of the "personal" nature of the data, is personal. This definition may provide protection for the most extensive area of personal information, as well as for the personal information that can be obtained through the combination of non-personal or anonymous data. In this case, as noted by B. Schneier, seemingly anonymous non-personal data will be turned

[198] Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 20 December 2017, Peter Nowak v. Data Protection Commissioner. Case C-434/16, para. 34.
[199] MALGIERI, Gianclaudio. Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data. *Privacy in Germany*, Vol. 2016, No. 4, 2016, p. 133; DE FRANCESCHI, Alberto; LEHMANN, Michael. Data as a Tradeable Commodity and New Measures for their Protection, *The Italian Law Journal*, Vol. 1, No. 1, 2016. pp. 51-52.
[200] JANEČEK, Václav. Ownership of Personal Data in the Internet of Things. *Computer Law and Security Review*, 2018, Vol. 34, No. 5, pp. 1039-1052.

into personal data.[201] But this blurring of the line between personal and non-personal data makes the GDPR, as N. Purtova calls it, "the law of everything".[202] In addition, it goes to the other extreme: if the right enshrined in Article 8 of the CFR protects personal information, regardless of its source, what does Article 7 of the CFR protect? On the other hand, the definition still indicates that information that is personal data is protected. This means that it is more certain to assume that the GDPR does not protect personal information, but rather the personal data itself.

The case practice of the ECtHR also shows that personal data itself is protected. For example, the ECtHR indicates that human DNA or human cell samples[203] contain a significant amount of unique personal data",[204] and their mere retention violates, without any further justification, the fundamental human right to privacy under article 8 of the ECHR.

In other words, even storing this data without any processing or interpretation already constitutes a violation of individual rights. This also shows that there are two types of personal data that are not completely uniform in their internal nature: there are personal data that always (by default) contain personal information and any interpretation of them leads to identification of the data subject's identity, and this is the main type of personal data defined by the GDPR, and there are personal data that do not have this intrinsic link with the person. If the protection of the former is related to conceptual and ethical issues, the protection of the latter is not. However, the protection of all personal data falls under the GDPR and it accepts the general concept of personal data, without making a distinction between personal data that contains personal information by default and data that is not. This means that the protection provided by the GDPR does not protect this internal link between personal data and the individual. Despite the fact that from the very beginning it seems that the GDPR protects the person, however, it rather protects the data itself, behind which the person is "not visible".[205]

B. "Relating to"

---

[201] SCHNEIER, Bruce. Why 'Anonymous' Data Sometimes Isn't. WIRED. [online]. 12th December 2007. [cit. on. 23th December 2023]. Accessible at: <https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/>.
[202] PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*. Vol. 10, No. 1, 2018, pp. 40-81
[203] ECtHR: Judgment of Grand Chamber of 4th December 2008. *S. and Marper v. The United Kingdom*. Nos. 30562/04 and 30566/04, para. *50.*
[204] Ibid, para. 75.
[205] URGESSA, Worku Gedefa. *The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging 'Data' as Exclusively Informational,* JIPITEC, Vol. 96, No. 7, 2016, p. 1.

"*Relating to*" is one of the elements of the definition of personal data that requires a context-sensitive assessment. In order to consider data as personal, it is necessary to first answer the question whether this information relates to a person, and even before conducting an identifiability analysis. "*Information relating to*" an individual can be interpreted broadly and narrowly and requires judgment about what type and degree of connection of information with a person is significant, as well as whether this connection is present at all.

The GDPR does not provide any guidance on how "*relating to*" should be understood. WP29 points out that "*relating to*" "is crucial as it is very important to precisely find out which are the relations/links that matter and how to distinguish them".[206] In some situations, this connection is obvious, while in others there is no connection. In particular, when the information relates to an object, for example, the value of a house, or a process or event requiring human intervention. In these cases, there will be an indirect relationship to the people who own the object or otherwise interact with it. In all cases, the assessment must take into account all the circumstances of the case.[207] WP29 expressed the view that data may "*relate to*" an individual because of (a) their actual content; (b) the purpose for which they are used; (c) the result or impact that this has on an individual.[208] The meaning of the word "*relating to*" becomes even broader if we consider that these three conditions are meant as alternative, and not as cumulative.[209]

Information about a person when its content is addressed directly to that person or concerns his/her personality, actions, characteristics or life experience. However, even information that does not relate to anyone in any way may turn out to be *"relating to"* a person. The information relates to a person for the purposes, "when the data are used or are likely to be used [...] with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual"[210] or when "[its] use is likely to have an impact on a certain person's rights and interests".[211] Moreover, such an impact is considered sufficient, "if the individual may be treated differently from other persons as a result of the processing of such data".[212]

It is noteworthy that the connection between the purpose and the result will occur not only when the data is already being used, but also where it is likely to be used for the purpose or effect of influencing people, "taking into account all the circumstances surrounding the

[206] Article 29 Working Party, Opinion 8/2010 on Applicable Law, pp. 9-10.
[207] Ibid.
[208] Ibid, p. 11.
[209] Ibid, p. 9.
[210] Ibid, p. 10.
[211] Ibid, p. 11.
[212] Ibid.

precise case".[213] In this context, a wider range of identification is used than in the standard Recital 26. In the modern world, any information can be associated with a specific person for its purpose, and all data can impact a person through various influences. Most of the information is processed for the purpose of evaluating, influencing the status or behaviour of people, which is described in WP29. For example, the adaptation of communications or the influence on human behaviour are key reasons for the collection and processing of information on the Internet. Thus, according to WP136, the term includes information about an individual, according to which information can also relate to an individual not because of its content, but because of the purpose or effect of its processing.

However, in the judicial practice of the CJEU the approach is somewhat different. So, in the case of *YS and others*[214] the Court adopted a limited interpretation of the term "relating to". The Court rejects the understanding of the term "*relating to*" in terms of the relationship of purpose and effect. It is important to note that this decision does not prohibit the use of a broader interpretation of "*information relating to*", as it does not apply to situations that, although they include information for assessment, differ from the facts considered in *YS and others* and similar cases.

In the case of *Nowak v. Data Protection Commissioner,* the Court revised the meaning of the term "*information concerning*". First, the CJEU confirmed that the concept of "personal data" potentially covers any information if it "*relates*" to the data subject,[215] including if the information is related to a specific person "*by virtue of its content, (...) purpose or effect"*. [216] The Court considered the connection between the information and the exam candidate to be significant, since the candidate's answers and the examiner's comments relate to the data subject in three aspects: they reflect information about the candidate (his knowledge, thought process and, in the case of a handwritten answer, information about his handwriting, as well as the examiner's opinion regarding the candidate's speech); the purpose of their processing – evaluate the candidate in terms of his professional abilities; and the use of this information may "have an effect on his or her rights and interests".[217] The Court also did not find it

[213] PURTOVA, Nadezhda. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. Law, Innovation and Technology, Vol. 10, No. 1, 2018, pp. 40–81.
[214] The Court of Justice of the European Union: Judgment of the Court (Third Chamber), 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, Case C-141/12.
[215] Judgment of the Court (Second Chamber) of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, Request for a preliminary ruling from the Supreme Court. Case C-434/16, para. 34.
[216] Ibid, para. 35.
[217] Ibid, para. 39.

problematic that the examiner's comments also concern him. The same information can relate to several persons, provided that they are identified.[218]

Secondly, the Court ruled that the status of the information as personal data "cannot be affected […] by the fact that the consequence of that classification is, in principle, that the candidate has rights of access and rectification".[219] The exam candidate has a legitimate interest, based on the protection of his privacy, in exercising his rights of access, rectification and objection in accordance with data protection law in relation to his or her answers and comments of the examiner. The right to delete data can also be used, and responses and comments destroyed, when the processing of information in an identifiable form is no longer required for the purposes for which the information was collected, for example, after the verification procedure is completed and cannot be challenged.[220] Thus, granting the candidate access rights in accordance with the GDPR serves the purpose of the GDPR, i.e. "guaranteeing the protection of that candidate's right to privacy […], irrespective of whether that candidate does or does not also have such a right".[221] The last point is in direct contradiction with the previous Court judgment in the case of *YS and others*.[222]

In the *Google Spain* case, the Court adopted a similar broad approach to control over search engine providers and personal data uploaded to third-party websites, arguing that a narrow interpretation would be contrary to the purpose of the DPD "is to ensure […] effective and complete protection of data subjects",[223] even in a situation where personal data is uploaded to a third-party website and the controller does not know this data.

The broad material scope of European data protection legislation makes data protection applicable to almost everyone who processes almost any information at almost any time.

C. "Identified or identifiable"

In order to be considered "personal data", the information must relate to an identified or identifiable person. Article 4(1) of the GDPR explains that a person can either be identified

---

[218] Ibid, para. 37-43.
[219] Ibid, para. 46.
[220] Ibid, para. 55.
[221] Ibid, para. 56.
[222] The Court of Justice of the European Union: Judgment of the Court (Third Chamber), 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, Case C-141/12.
[223] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12, para 34.

directly or indirectly and provides a non-exhaustive list of so-called "identifiers".[224] WP29 adopts a broad understanding of this element. "*Identified*" refers to a person who is known or distinguished in the group, and "*identifiable*" is a person whose identity has not yet been identified, but identification is possible.[225]

The standard for the appropriate identification capability in WP29 is whether the means of identification are "reasonably likely to be used". The Recital 26 of the GDPR defines a test for a reasonable probability of identification, taking into account the level of technology development at the time of processing: *"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".*

WP29 states that the means of identification are *"reasonably likely to be used by the controller or any other person"*, which is often interpreted as *by anybody,*[226] which is a much broader interpretation, allowing more data to be considered personal, that a *"purely hypothetical possibility"* of identification is insufficient to meet the standard of *"reasonably likely"*.[227] To assess this possibility, one should take into account *"all the factors at stake"*.[228] The standard of reasonable probability of identification is quite broad and as a result "[r]ecital 26 GDPR makes the GDPR concept of 'personal data' suitable for 'a tailored, context-specific analysis for deciding whether or not personal data is present'".[229] The same data can be anonymous at the time of collection, but later turn into personal data simply by being there

[224] Recital 24 further cites examples of online identifiers which 'may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them.'. From a technical perspective, it is worth highlighting that 'any information that distinguishes one person from another can be used for re-identifying data.'; See also NARAYANAN, Arvind, SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiable Information". *Communications of the ACM*, 2010, Vol. 53, No. 6, p. 24.
[225] Article 29 Working Party, Opinion 8/2010 on Applicable Law, p. 12
[226] TAYLOR, Mark. Genetic Data and the Law: A Critical Perspective on Privacy Protection, Cambridge: Cambridge University Press, 2012, 140 p.; URGESSA, Worku Gedefa. The Protective Capacity of the Criterion of Identifiability under EU Data Protection Law. European Data Protection Law Review, Vol. 2, 2016, p. 521.
[227] Article 29 Working Party, Opinion 8/2010 on Applicable Law, p. 15.
[228] Ibid, pp. 15–16.
[229] SCHWARTZ, Paul M., SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 2011, Vol. 86, p. 1814.

due to technological progress. Some scholars agree that the meaningful difference between identifiable and unidentifiable information will no longer be sustainable.[230]

The Court considered the meaning of the word *"identifiable"* in the judgment of the *Breyer* case. The central issue before the Court was whether a dynamic IP address represented information related to an identifiable person in relation to the website provider, if the additional data needed to identify the website visitor was held by the visitor's Internet service provider.[231] The Court followed a broad interpretation of identifiability, but narrowed the scope of the concept of "personal data". The CJEU concluded that in order to be considered personal data, it is not necessary that the information itself allows the identification of the data subject or "that all the information enabling the identification […] must be in the hands of one person".[232] The Court offered to evaluate, "whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject".[233] The Court took into account the Advocate General's (AG) argument that the possibility of combining a dynamic IP address with additional data would not be reasonably likely if it were "prohibited by law or practically impossible" due to "disproportionate effort in terms of time, cost and man-power".[234] It was found that the website provider has tools that can be used with sufficient probability to identify website visitors based on a dynamic IP address with the help of third parties, namely the Internet service provider and the competent authority.[235] Thus, dynamic IP addresses turned out to be personal data.

The Court's position on the question of which means of identification can be reasonably used among the factors indicated by WP29 also indicated the factor of legality: identification would not be "likely reasonably" if it were prohibited by law. This directly contradicts WP136. This can potentially limit a number of situations where data is considered identifiable. However, in general, the *Breyer* case confirmed the broad interpretation of WP29: "all the means "likely reasonably" to be used for identification (either by the controller or by any third party)".[236]

D. "Data processing"

---

[230] For example, see FINCK, Michèle, PALLAS, Frank. They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR. International Data Privacy Law, 2020, Vol. 10, No. 1, pp. 11–36.
[231] Judgment of the Court (Second Chamber) of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland,* C-582/14. para. 39.
[232] Ibid, para. 43.
[233] Ibid, para. 45.
[234] Ibid, para. 46.
[235] Ibid, para. 46 - 49.
[236] Ibid, para. 42.

According to Article 3(3) of the GDPR, "*processing*" is any operation or set of operations that are performed with personal data, regardless of whether they are automated or not, such as collection, recording, organization, structuring, storage, adaptation or modification, search, consulting, use, disclosure by transmission, distribution or otherwise granting access, alignment or combination, restriction, erasure or destruction. That is, the GDPR provides a non-exhaustive list of examples explaining what such operations can entail, and there is no difference between the collection and use of information, regardless of the methods used, the intensity or frequency of operations. As the CJEU points out in the *Lindqvist* and *Google Spain* cases, even the most insignificant data processing operation can quickly have a more or less significant impact on the data subject.[237] In the *Google Spain* case, the Court rejected Google's argument that its activities cannot "be regarded as processing of the data which appear on third parties' web pages displayed in the list of search results, given that search engines process all the information available on the internet without effecting a selection between personal data and other information".[238] That is, it does not matter whether a certain operation involves the processing of personal data. The lack of a requirement of intent is particularly evident in light of data protection requirements. This approach also includes actions to erase, encrypt or anonymize personal data in the concept of "*processing*" and therefore in the scope of the GDPR.

Thus, processing in the context of the GDPR is a concept that covers all actions that a person can perform with personal data. Each of these processing operations individually must comply with GDPR requirements and non-compliance may lead to the application of the rights of the data subject, such as the right to erasure.

On the other hand, Articles 10 and 19 of the GDPR impose on data controllers the responsibility for processing data related to criminal convictions or offenses only in accordance with official authority, such as a data protection officer. But, as the main and essential source of law, Article 11 of the CFR allows freedom of expression to be exercised regardless of any borders and state authorities, which clearly shows the difficulty of determining the legality of processing. Depending on the issues and principles in question, it is clear that this is a matter

[237] See, for example: *Lindqvist,* para. 268; The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12, para. 24.

[238] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12, para. 23-24, 28-31.

of purely contextual definition, which must be carried out in accordance with the motives and provisions of the law.

The processing principles applied by the CJEU, the ECtHR and the GDPR can be interpreted as a mechanism to achieve balance through gradual development. Because one thing is common to all actions that are carried out in accordance with the law or the grounds for the legality of data processing. By setting the legality parameter, the CJEU introduced terms such as "inadequate, irrelevant or excessive in relation to the purposes of the processing".[239] In addition, both the CJEU and the ECtHR have legalized the processing for archiving data for public use in scientific or historical research. Public protection is ensured by allowing processing also on the basis of exercising freedom of expression. And public rights are protected if it is consistent with the principles established by law, meets the goals of fundamental protection and corresponds to the values of a democratic society. Now the provisions of the law are clear with the application of the GDPR, which defines the scope of the legality of processing in its specific articles. However, when interpreting the principles of case law arising from both the CJEU and the ECtHR in cooperation with the GDPR, some principles were repealed with the enactment of the GDPR, which were established within the framework of the directive regime. For example, when prioritizing public and private interests, it is assumed that both the instructions and the discretionary powers of Member States to adopt national regulations in accordance with personal social values and traditions are being eroded and replaced.

The GDPR has only expanded the scope of application from the search engine to the controller, but has not developed any draft defining who is responsible for cross-checking these balancing measures, which should be effective enough to respect the right to privacy and personal data of convicts in each case. Perhaps this is done in order to take into account the best practices that should be adopted to face the issues and challenges ahead.

At the moment, while the GDPR may be the hegemon regarding the legality of processing, it lacks the proper balance, especially with regard to convicts serving sentences. Now, one can say that the solution has begun to fill in the gaps by setting out the principles, but after the widespread application of the GDPR, more needs to be done to preserve data protection.

---

[239] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12., para. 92-94.

4.3 The scope of data protection and the problem of disproportionate legal consequences

Despite the fact that the CJEU prefers a broad interpretation of the elements of personal data, however, an overly broad interpretation can lead to problems delineating the scope of the data protection Act. The CJEU pointed out that an overly broad interpretation of the scope of the DPD would lead to unreasonable and disproportionate results. For example, in the *Lindquist* case, the Court considers it unreasonable to assume that "the mere mention by name of a person or of personal data in a document [...] on an internet page constitutes automatic processing of data".[240]

In the *Google Spain* case, AG Jääskinen stated that "the broad definitions of personal data, processing of personal data and controller are likely to cover an unprecedently wide range of new factual situations [...]. his obliges the Court to apply [...] the principle of proportionality, in interpreting the scope of the Directive in order to avoid unreasonable and excessive legal consequences".[241] However, the Court did not recognize that proportionality must be taken into account at the stage of determining the scope of the DPD. The Court only pointed out that rather the DPD itself has a certain degree of flexibility.[242] In fact, the principle of proportionality is secondary to the issue of the scope of application.[243] In the *Google Spain*, the Court did not accept the proportionality argument, given the purpose of the Directive "seeks to ensure a high level of protection of the fundamental rights and freedoms [...] with respect to the processing of personal data",[244] and that, since the provisions of the DPD can "infringe fundamental freedoms", they must be interpreted in the light of fundamental rights.[245]

The GDPR, although considered a receiver of the DPD, nevertheless pursues a broader, "Janusian" goal – to ensure an equal level of protection for individuals and the free flow of personal data throughout the EU and thus contribute to the functioning of the internal market.

---

[240] Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist, Case C-101/01. para. 20.
[241] Opinion of Advocate General Jääskinen, delivered on 25 June 2013, para. 30.
[242] Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist, Case C-101/01. para. 83.
[243] Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist, Case C-101/01. para. 87–88.
[244] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12., para. 66.
[245] For a general discussion of the judgment see LYNSKEY, Orla. Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. Modern Law Review 522. Vol. 78 No. 3., 2015, pp. 522-534.

It should be noted that the GDPR text itself does not consider the protection of individuals as a restriction on the movement of personal data. In accordance with Article 1(3) of the GDPR: "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".

The "two-faced" feature of the legal act shifts the burden of choosing telos onto the shoulders of the case law of the CJEU. And the CJEU considers the goal of promoting the formation of the internal market in the adopted hybrid GDPR model to be secondary in its practice and gives priority to the goal of protecting the rights of individuals. In the cases of *Schrems II*, [246] *Wirtschaftsakademie* [247] and *FashionID*, [248] the Court has already formed approaches to the predictability of the subsequent application and interpretation of the GDPR, namely in order to protect the rights of individuals. The Court's judgment in *Google v. CNIL* even allows for the continued application of the right to be forgotten worldwide and is seen as an attempt to develop progressive case law to protect human rights in the digital age (the specified case will be discussed in more detail in another chapter).[249] It should be noted that the CJEU has an enviable consistency of interpretation in the context of protecting the fundamental right to data protection. And this sequence does not change after the adoption of the GDPR and in judicial practice after *Google Spain* case. Thus, the Court's position is that any possible undesirable impact of the widespread application of the EU data protection law should be mitigated by proportionately applying specific provisions in the context of protecting the specified purpose. The case law on certain elements of the concept of "personal data" largely fits into the same model. This requirement interprets the provisions of the GDPR in the context of effective protection of individuals and is aimed at preventing legal loopholes in order to guarantee effective and complete protection of data subjects.[250]

---

[246] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. Case C-311/18.
[247] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH,* Case C-210/16.
[248] The Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 29 July 2019, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV,* Case C-40/17.
[249] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 September 2019. *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL).* Case C-507/17.
[250] See in this regard: LYNSKEY, Orla. The Foundations of EU Data Protection Law. Oxford: Oxford University Press. 2015. 336 p.

5 Finding a balance between the right to be forgotten and freedom of expression

This section focuses on the aspects of finding the necessary balance of rights between the right to be forgotten and freedom of expression. The freedom of expression is recognized in most international human rights treaties, including the Universal Declaration of Human Rights (Article 19),[251] International Covenant on Civil and Political Rights (Article 19),[252] African Charter on Human and Peoples' Rights (Article 9),[253] American Convention on Human Rights (Article 13)[254] and European Convention on Human Rights (Article 10).[255]

In General comment No. 34, the UN Human Rights Committee (HRC) confirmed that freedom of expression is essential for the enjoyment of other human rights and stressed that article 19 of the International Covenant on Civil and Political Rights (1966) protects all forms of expression and means of dissemination, including all electronic means. [256] The Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines dated April 4, 2012 emphasizes the importance of search engines to facilitate access to Internet content and ensure the usefulness of the World Wide Web to the public. The CMCE considers it necessary for search engines to be able to freely explore and index information that is available on the Internet and intended for mass distribution. The Recommendation also notes that the actions of search engines may, however, affect freedom of expression and the right to seek, receive and disseminate information, as well as the right to respect for privacy and protection of personal data due to the prevalence of search engines and their ability to penetrate and index content that, although in public space, but it was not intended for mass communication. [257]

After the adoption of the Lisbon Treaty, the rights in question received the status of fundamental human rights, and after the adoption of the GDPR, the freedom of expression was

---

[251] Universal Declaration of Human Rights (10 Dec. 1948), U.N.G.A. Res. 217 A (III) (1948).
[252] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.
[253] Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).
[254] Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969
[255] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.
[256] UN Human Rights Committee (HRC), *General comment no. 34, Article 19, Freedoms of opinion and expression*, 12 September 2011, CCPR/C/GC/34.
[257] Council of Europe: Committee of Ministers, Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, 4 April 2012.

prescribed as one of the reasons for restricting the right to be forgotten. In accordance with Article 17(2) of the GDPR, the right to be forgotten does not apply to the extent that the processing of personal data is necessary for the exercise of the freedom of expression. The current state of the right to be forgotten and freedom of expression cause balancing problems and the need for such balancing has been repeatedly pointed out both in the judicial practice of the ECtHR and the CJEU.[258]

5.1 Balancing the *Google Spain* case

In the *Google Spain* case, the Court stressed that the right enshrined in the Article 17 of the GDPR cannot be considered as unlimited: "as the de-referencing of search results might negatively affect others, e.g. internet users trying to obtain information on a past event, such requests have to be carefully weighed against the latter's freedom of information".[259] This clearly indicates possible problems in balancing this right with other rights and interests in the law-enforcement practice. Therefore, the CJEU in its judicial practice tries to consistently form an acceptable balancing position and provide the most possible level of protection of the right to data protection while respecting other rights and interests.

The CJEU in the *Google Spain* case noted an important condition for the existence of the right to be forgotten - it will cease to exist if it is not balanced with the freedom of expression. The Court emphasizes the priority of the right to oblivion over the economic interests of search engines and the public interest in personal information. The Court points out that the right to respect for private life, as a rule, overrides the economic interest of the search engine operator, and the interest of an individual in deleting personal data in accordance with Articles 7 and 8 outweighs the public interest in accessing his/her information in accordance with Article 11 of the CFR.[260] The CJEU further notes that this general rule should not be applied if there is a prevailing interest of the general public in access to information "for particular reasons, such as the role played by the data subject in public life".[261]

---

[258] Judgment of the Court (Grand Chamber) of 29 January 2008. *Productores de Música de España (Promusicae) v Telefónica de España SAU*. C-275/06. pp. 309-348.

[259] GLOBOCNIK, Jure. The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17). *GRUR International*. Vol. 69, No. 4, 2020, pp. 380-388.

[260] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12., para. 1-21.

[261] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12., para. 97, 99.

However, the wording given by the Court in the *Google Spain* case did not resolve the issues of contradiction between the rights in question. Firstly, the prevailing interest of the general public in access to information is not due solely to the role of the data subject in public life, this is only one of the possible reasons, but there may be other "special reasons" similar in importance or substance to the role indicated by the CJEU. The permissibility of possible situations does not make it possible to unambiguously decide how much weight one right should have in relation to another.

Secondly, the CJEU has not developed any criterion for determining the priority between the "public interest" and the "right to be forgotten" when public and private interests compete, especially when there is no direct separation between public and private interests. This problem remains unresolved, especially after the GDPR mentions freedom of expression as one of the derogations from the right to be forgotten. In general, mentioning only one right as a limiter of the right to be forgotten has become one of the problems in the balancing issue, especially when, according to Article 85 GDPR balancing between rights is one of the goals of the GDPR. The contradiction lies in the fact that the GDPR prescribes the freedom of expression and information as one of the derogations from the right to be forgotten in accordance with Article 17(3)(a) of the GDPR. According to Recital 19 and Article 10 of the GDPR, one of the goals is to protect the fundamental freedoms and rights of convicts. In addition, Article 10(2) of the ECHR defines the protection of the reputation and rights of others as one of the reasons for restricting freedom of expression. And it seems that since the right to be forgotten has the effect of protecting the reputation and rights of others, balancing becomes inevitable and this may impose restrictions on freedom of expression.

Thirdly, the Court only mentioned the principle of a public figure, according to which the applicant's social status or public activities of the applicant may generate public interest, which may outweigh the right to be forgotten. Although the *Google Spain* judgment says that any public-related work is in the public interest, however, what are the factors that make certain actions or certain persons public? In addition, the CJEU ruled that search engine data controllers may be required to remove links that lead to anyone who searches for information by name on the website where the data is posted, according to the DPD.[262] Thus, the CJEU came into

[262] Information Commissioner's Office. Data Protection Act of 1998 Supervisory Powers of the Information Commissioner Enforcement Notice [online], 2015. [cit. on 27th December 2023]. Accessable at: <https://ico.org.uk/media/action-weve-taken/mpns/2259545/ams-marketing-ltd-mpn-20180727.pdf>.

conflict with Article 6(1)(b) of the DPD according to which the processing of data for archiving purposes in the public interest, statistical, scientific or historical research purposes is allowed.[263] Fourthly, in determining the right to be forgotten, the Court distinguished the right only within the framework of search, which is carried out through search engines, and not in a broader sense. This means that data erasure is only possible in relation to search engine listings, while the information itself may remain on the Internet. That is, according to the Court, the right to be forgotten is rather the right to restrict data search, and as P. Bernal notes, the Court's judgment did not reach the milestone that, in the opinion of many researchers, it crossed.[264]

Thus, the CJEU maintains that the priority of the right to be forgotten can be reconsidered if it concerns public figures, but EU law allows rejecting a request for the right to be forgotten if it violates freedom of expression, as stated in Article 17(3)(a) GDPR.

5.2 Doctrinal Balancing Discussion after the *Google Spain* case

After the judgment in the *Google Spain* case, even more acute discussions began on the problem of balancing the two rights in question. Thus, sceptics argued that the judgment of the CJEU put the right to respect for private life above other rights. S. Peers points out that by focusing on the right to respect for privacy, the EU forgot that other rights and guarantees were also applicable.[265] M. Husovec notes that by creating a presumption regarding the right to erasure, the CJEU has created a "super-human [] right",[266] although there is no hierarchical connection between the conflicting human rights.[267] D. Drummond expressed the opinion that the CJEU gave priority to the right to be forgotten, sacrificing the rights to freedom of expression, which also have a similar status in CFR.[268] AG N. Jääskinen stresses the need for freedom of

---

[263] The European Parliament and the Council of European Union. EU Directive 95/46: Directive 95/46/EC of the European Parliament and of the Council of 24 October on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ 1995 L 281/31; 1995: 31–50.

[264] BERNAL, Paul A.. A Right to Delete?. *European Journal of Law and Technology*, Vol. 2, No. 2, 2011, pp. 1-18.

[265] PEERS, Steve. The CJEU's Google Spain Judgment: Failing to Balance Privacy and Freedom of Expression, EU Law Analysis. [online]. 13th May 2014 [cit. on. 25th December 2023], Accessible at: <http://eulawanalysis.blogspot.co.uk/2014/05/the-cjeus-google-spain-judgment-failing.html [http://perma.cc/T8QN-W2G2]>.

[266] HUSOVEC, Martin. Should We Centralize the Right to Be Forgotten Clearing House? Center for Internet and Society [online]. 30th May 2014, [cit. on. 25th December 2023]. Accessible at: <https://cyberlaw.stanford.edu/blog/2014/05/should-we-centralize-right-be-forgotten-clearing-house>.

[267] Ibid.

[268] DRUMMOND, David. We Need to Talk about the Right to Be Forgotten. London: The Guardian [online]. 10th July 2014. [cit. on. 25th December 2023]. Accessible at: <https://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate>.

expression in the EU and expresses the greater power given to data controllers to take initiatives to balance complex competing rights.[269]

Other scholars, on the contrary, do not see the problem in balancing these rights. Thus, G. Frosio believes that the myth that the right to be forgotten damages freedom of expression should be repressed once and for all. The right to be forgotten does not burden freedom of expression in any other way than the traditional right to respect for privacy/freedom of expression dichotomy used in European law.[270] J. Ausloos and A. Kuczerawy, in turn, note that the debate about the right to be forgotten concerns data protection as opposed to economic interests, not freedom of expression.[271] S. Colliver argues that not all rights should be compatible and this conflict between the two rights does not harm the survival of either of them.[272]

Some scholars associate the problem of balancing the rights in question with the legal system. L. Floridi and M. Taddeo point out that establishing the right balance between them is not an easy task. According to the European approach, the right to respect for private life trumps freedom of speech, while the American point of view is that freedom of speech is predominant in relation to the right to respect for private life. Thus, determining the responsibility of online service providers in relation to the right to be forgotten turns out to be a very difficult process, since it involves balancing various fundamental rights, as well as considering the relationship between national and international law.[273]

"Article 19" has developed a number of recommendations to ensure an appropriate balance between the right to be forgotten and freedom of expression:

1. The right to be forgotten must be strictly limited, since certain minimum requirements must be met in order for such a right to be compatible with the right to freedom of expression, both from the point of view of substance and from the point of view of procedural aspects of its implementation. In particular, the right to be forgotten should be limited to individuals and should apply only to search engines (data controllers), and not to hosting services or content providers. Any protection must also contain an explicit reference to freedom of expression as a fundamental right, with which the right

[269] Opinion of Advocate General Jääskinen, delivered on 25 June 2013, para. 27.
[270] FROSIO, Giancarlo F. The Death of 'No Monitoring Obligations': A Story of Untameable Monsters, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 8, No. 3, 2017, p. 335.
[271] KUCZERAWY, Aleksandra, AUSLOOS, Jef. From notice-and-takedown to notice-and-delist: Implementing Google Spain. *Colorado Technology Law Journal*, Vol. 14, No. 2, 2016, p. 220.
[272] BEAUMONT, Paul. Striking a Balance: Hate Speech, Freedom of Expression and Non-Discrimination. *International and Comparative Law Quarterly*. 1994, Vol. 43 No. 2, pp. 476-478.
[273] FLORIDI, Luciano, TADDEO, Mariarosaria, What is Data Ethics? *Philosophical Transactions of the Royal Society A*, Vol. 374, No. 2083, 2016, p. 1592.

to be forgotten must be balanced. In addition, decisions on requests for the right to be forgotten should be made only by courts or independent judicial authorities.

2. Seven criteria should be applied to establish a balance between the right to freedom of expression and the right to be forgotten:
   a. Is the information in question private;
   b. Did the applicant have a reasonable expectation of confidentiality, including consideration of issues such as prior conduct, consent to publication, or prior existence of information in the public domain;
   c. Does the information in question meet the public interest;
   d. Does the information in question relate to a public figure:
   e. Is this information part of a public record;
   f. Has the applicant suffered significant harm;
   g. How relevant is the information and does it remain of public importance.[274]

These recommendations, however, do not fully find their expression in the judicial practice of the CJEU. For the most part, they express the approaches reflected in the practice of the ECtHR. Thus, the theoretical basis of the ECtHR's argument is focused on ensuring a balance between the right to public discussion and the serious damage caused by publication.[275] On the contrary, in the *Google Spain* case the CJEU suggested that a violation of an individual's rights could be established even if the individual concerned had not suffered any damage.

5.3 Right to be forgotten and freedom of expression balancing approaches of the CJEU and the ECtHR

5.3.1 The CJEU: harmonization of balancing with the prefix "dis-"

Balancing the tension between freedom of expression and the right to be forgotten is a difficult task due to the existence of many connotations that require balancing. Both rights must be combined and exist in parallel, that is why the CJEU from the very beginning sought to find a balance between them, paying equal attention to both. In the case of *Satakunnan Markkinapörssi Oy ja Satamedia Oy* the Court indicates that none of the competing interests

[274] Article 19. The Right to be Forgotten: Remembering Freedom of Expression. [online]. 2016 Accessible at: <https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_ HYPERLINKS.pdf>.
[275] See the cases of *Tamiz v. United Kingdom* and *Einarsson v. Iceland.*

are exclusive, both of them can be limited if appropriate grounds are found, consistent with the law, serving the purpose of ensuring rights and, equally importantly, corresponding to the democratic merits of a particular legal system or society.[276] However, it is also obvious that the use of the same mechanisms can lead to a conflict between these rights, which confirms the opinion of the CJEU in the *Bodil Lindqvist* case that "gauge of weighing between those contradictory rights race against each other within the ambit of the contemporary data protection enactment".[277]

The DPD provided Member States with the freedom to choose the appropriate approach in accordance with their domestic obligations in order to ensure a balance between rights in the absence of synchronous guidance in accordance with the law. In the case of *Institut Professionnel Des Agents Immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte,* the CJEU pointed out that Article 13 of the Directive gives Member States the freedom to formulate their legislative acts indicating restrictions on the right of people to information.[278] The GDPR also transfers an effective balancing mechanism to the national legislator, giving Member States the authority to adopt national data protection laws through Articles 2, 23 and 85 of the GDPR. These provisions, however, create differences in the application of the law. Some local legal norms, along with article 17(3) of the GDPR, include grounds for derogation, which leave members the opportunity to allow processing in accordance with any of these specific principles (Germany, Finland). This makes it difficult for the CJEU to provide uniform initial interpretations at the EU level. On the other hand, EU law provides some opportunity to determine the scope of the right to be forgotten by the national legislator. Thus, the GDPR did not take into account the Court's opinion on the need to unify approaches so that better harmonization could be achieved by providing guidelines for weighing competing interests.[279]

In the *Google Spain* case, the Court emphasized the need to take into account different interests, considering the impact of specific information on personal life, balancing privacy interests such as right to delete and publicity interests such as the monetary benefit of the search engine, the performance of a public role by the data subject or the exercise of freedom of

[276] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 16 December 2008. *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*. Case C-73/07.
[277] FAISAL, Kamrul. Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions. SECURITY AND PRIVACY, 2021, Vol. 4, no. 4, p. 157
[278] The Court of Justice of the European Union: Judgment of the Court (Third Chamber) of 7 November 2013, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, C-473/12., para. 1–10.
[279] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 16 December 2008. *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*. Case C-73/07.

expression.[280] However, the Court has not developed any criteria for this consideration. The analysis of EU case law shows that the Court gives only some guidance on the definition of public interest for balancing purposes. Thus, in the case of *GC, ED and others*, the CJEU clarified that the publication or further processing of data and the freedom of expression should exclude the processing of confidential information or information of a special category, unless otherwise specified in the law. [281] In the case of GC, the article was related to the applicant's political beliefs and orientation. She was a public figure whose activities were related to the public. In other words, ordinary people were interested in learning about her because she participated in the provincial elections. But it is necessary to emphasize the fact that the information was made public at a crucial moment when she was conducting her election campaign. Journalism is clearly damaging her public image. Moreover, she is no longer connected to her previous profession. In this situation, her right to privacy should be respected only if the information about a personal relationship is nothing but a lie.

In the case of ED, who was convicted of sexually abusing children under the age of 15, Article 10 of the GDPR prohibits the processing of criminal data without the control of official authorities. Although the law provides for the erasure of criminal record data, other factors compete to detract from this, such as the nature of the crime. For example, if ED starts performing duties in institutions that offer their activities to children, then ordinary people will have a legitimate interest in previous criminal activities. Thus, the CJEU does not give clear instructions to Member States, but rather encourages national courts to find a balance between rights, which contradicts the harmonization of EU legislation.

5.3.2 The right to be forgotten: the expansion of the right in the "post-*Google Spain*" case-law of the ECtHR

The ECtHR stressing the importance of the right to respect for privacy and freedom of expression as 'one of the essential foundations of a democratic society',[282] confirms that Article 10 of the Convention is fully applicable to the Internet. Prior to the *Google Spain* case, the ECtHR was very reluctant to recognize the right to erasure of news reports published in the past

[280] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12., para. 1-21.
[281] Article 9 of the GDPR defines special categories of data that are associated with the expression of "racial or ethnic origin, political views ...".
[282] For example, see the cases of *Von Hannover v. Germany (№ 2)* and *Axel Springer AG v. Germany*.

because of their public interest. Thus, in the case of *Węgrzynowski and Smolczewski v. Poland* [283] and in the case of *Fuchsmann v. Germany,*[284] the ECtHR concluded that news archives, including online archives "constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free"[285] and their function deserves protection. Therefore, in both cases, the Court concluded that there had been no violation of article 8 of the Convention.

In the case of *ML and WW v. Germany*[286] The ECtHR has considered a request for anonymization of personal data contained in newspaper articles and stored in digital media archives. The applicants convicted of murder believed that the availability of these articles in online archives had the effect of constant stigmatization. The ECtHR concluded that there had been no violation of article 8 of the Convention, since in this particular case the reports available online continued to contribute to a discussion of public interest that had not diminished over time. The Court argued that journalists are free to decide which details should be published in the media. Thus, the Court concluded that the applicants had only a limited legitimate expectation of anonymity in the reports. As for the right to be forgotten, the Court did not refer to it at all.

The ECtHR has developed an extensive practice on balancing these rights. In the cases of *Von Hannover v. Germany* and *Axel Springer AG v. Germany*[287] the ECtHR has established the following criteria for balancing:

1) the contribution of the article to the debate of public interest;
2) the degree of fame of the person and the purpose of the article;
3) the behaviour of a person relying on the right to be forgotten in relation to the media;
4) the method of obtaining information and its reliability;
5) the content, form and impact of the publication;
6) the severity of the measure imposed on the publisher.

Thus, the ECtHR does not recognize by default the priority of any of these rights, as the CJEU does in the *Google Spain* case.

However, the real triumph of the right to be forgotten began with the case of *Sanchez v. France*, the decision on which was assessed as "another drop in the dilution of

[283] ECtHR, Fourth Section, *Węgrzynowski and Smolczewski v. Poland*, Application no. 33846/07, July 16, 2013.
[284] ECtHR, Fifth Section, *Fuchsmann v. Germany*, Application no. 71233/13, October 19, 2017.
[285] ECtHR, Fifth Section, *Fuchsmann v. Germany*, Application no. 71233/13, October 19, 2017.
[286] ECtHR, Fifth Section, *M. L. and W. W. v. Germany*, Applications nos. 60,798/10 and 65,599/10, September 28, 2018.
[287] ECtHR: Judgment of 7 February 2012, *Von Hannover v. Germany (№ 2)*, App. nos. 40660/08 and 60641/08; ECtHR: Judgment of 7 February 2012, *Axel Springer AG v. Germany*, № 39954/08, para. 89.

the protection granted by the ECtHR to freedom of expression".[288] In this judgment, the ECtHR somewhat complicates the search for a balance regarding freedom of expression on the Internet, pointing to the possibility of criminal liability of a Facebook user for comments written by third parties. Julien Sanchez, mayor of Beaucaire (France), posted a post on Facebook about his political opponent during the elections. His supporters posted offensive comments to this post addressed to Muslim residents of the city. Sanchez and others who wrote the comments were accused of inciting hatred. Sanchez appealed to the ECtHR, claiming a violation of the freedom of expression. The ECtHR disagreed with the applicant's arguments. The ECtHR took into account the fact that the applicant deliberately made the wall of his Facebook account public, thereby allowing his subscribers to post comments there. The Court ruled that his status as a political figure required even greater vigilance on his part.

However, the present expansion and priority of the right to be forgotten has been noted by two so-called post-*Google Spain* judgments of the ECtHR – *Hurbain v. Belgium* and *Biancardi v. Italy*. [289] These judgments change the balance between Articles 8 and 10 of the Convention to give priority to the former. Moreover, the ECtHR, unlike the CJEU, expands the scope of the right to be forgotten. In EU law, deindexation cases focus on search engines, [290] and *Biancardi v. Italy* is the first case in which a request for de-indexing was granted in relation to the primary source, that is, the ECtHR allowed applicants to send their requests directly to the main publisher, and not to the search engine, even if it would have been enough for the search engine to remove the links.

In both decisions, the Court found that there had been interference with the freedom of expression, but this interference was provided for by law and pursued a legitimate purpose. The Court stressed that the interference was proportionate, since the news organization was not required to delete the full text of the relevant article from its internal archives, but only to cancel the indexing of the applicants' names.

The Court referred to the wide margin of discretion of the national courts while maintaining a balance between articles 8 and 10 of the Convention.[291] In the judgment of *Biancardi v. Italy* case, the Court provided additional recommendations on the application of

---

[288] ALKIVIADOU, Natalie. Hate Speech by Proxy: Sanchez v France and the Dwindling Protection of Freedom of Expression. OpinioJuris [online]. 14th December 2021. [cit. on. 25th December 2023]. Accessible at: <https://opiniojuris.org/2021/12/14/hate-speech-by-proxy-sanchez-v-france-and-the-dwindling-protection-of-freedom-of-expression/>.

[289] ECtHR: Judgment of 25 February 2022, *Biancardi v. Italy*, App. no. 77419/16.

[290] For example, see the cases of *Google Spain* and *Google v. CNIL*.

[291] ECtHR: Judgment of 16 June 2015, *Delfi AS v. Estonia*, App. no. 64569/09.

the *Alex Springer* test in an online context. The Court was faced with the following questions: a) whether the applicant's freedom of expression was violated as a result of being found responsible for refusing to de-index the material, and b) whether the obligation to de-index the material can be extended to administrators or journalists, and not limited to search engines (as in Google Spain). The Court repeated the criteria of *Axel Springer* case, but saw actual differences between this case and the *Alex Springer* case. The Court considered these criteria inappropriate and limited its consideration to three issues: the length of the article's stay on the website after the request, the confidentiality of data (related to the ongoing criminal proceedings) and the severity of the sanction ("not excessive"). With regard to the first paragraph, the Court noted that the article had not been updated since 2008, and over time the applicant's right to disseminate information was decreasing, while the plaintiff's right to respect for his private life and reputation was increasing (see *Plon v. France*).

According to paragraph 2, the Court found that confidential information, for example, related to criminal proceedings, is of great importance for establishing a balance between the dissemination of information and the right to privacy. Finally, the severity of the sanction was found to be "not excessive", since only civil liability was established, and the amount of damage awarded was proportional to the interference with the plaintiff's rights in accordance with Article 8. The Court found no reason to deviate from the balancing procedure conducted by the Italian court and ruled that the freedom of expression had not been violated by the decision against him.

Unlike the judgment in *Gheorghe-Florin Popescu v. Romania*, the Court did not emphasize as a "significant factor" that the applicant was a journalist and that freedom of the press performs a fundamental function in a democratic society, whereas in the practice of the CJEU and the GDPR exclude the processing of data solely for journalistic purposes from the scope of the right to be forgotten.

In the case of *Hurbain v. Belgium*, the Court shows which elements must be carefully studied when balancing in the online sphere. The Court recalls the six criteria of the *Axel Springer*'s case, but finds that the inclusion of an article in digital archives has a different effect on debates of public interest than its initial publication. The ECtHR recognized that the right to privacy does not provide a remedy for damage to a person's reputation caused by his own behaviour, but ruled that publication in online archives should not turn into a "virtual criminal record". In addition, G. was not a public figure and, with the exception of the article in question, the facts on which G. was convicted did not receive any media coverage. The Court ruled that the article discussed incidents that occurred in 1994, and a fragment in digital archives is more

likely to undermine the right to privacy and a different regime than that applied to traditional print media may be justified. The Court concluded that there was no violation of the right to freedom of expression and the scales tipped in favour of the right to be forgotten.

The Court has already considered the right to be forgotten in an online context in the case of *ML and WW v. Germany,*[292] where the Court considered the four criteria of the *Axel Springer* case to compare the freedom of expression with the right to privacy and did not take into account the last two criteria: 1) the method of collecting information in the article and the reliability of the facts, as well as 2) the seriousness of the measure imposed on the offender. The Court in this case also stressed "the essential role played by the press in a democratic society", and drew a distinction between the "amplifying effect" of search engines and the original publisher of information, "whose activity is generally at the heart of what freedom of expression is intended to protect". These approaches are changing in case of *Hurbain v. Belgium*.

In the *Hurbain v. Belgium* case, the ECtHR once again requires national courts to carefully examine all six criteria of the *Alex Springer*'s case, thereby returning to previous practice. However, at the same time, he emphasizes that in the online mode, some criteria of the *Alex Springer*'s case may be assigned different weights when balancing the rights in question, since digital archives may have a more detrimental impact on the human right to privacy than traditional print media. As a result, the ECtHR confirmed that balancing can lead to different results depending on the online or offline environment. So, earlier, both the CJEU and the ECtHR consistently distinguished between press websites and external search engines on the grounds that search engines have become the main source of information on the Internet, and thus limited the right to be forgotten by changing search results in search engines.

Having analysed the judicial practice of the ECtHR, it should be noted that the grounds referred to by the CJEU in its judicial practice, especially after the judgment in the *Google Spain* case, differ from the grounds referred to by the ECtHR when considering the right to be forgotten. The theoretical basis of the ECtHR's argument focuses on ensuring a balance between the right to public discussion and the damage caused by publication, and applying the standard of serious damage to assess damage - the damage caused must reach a certain level in order to become a significant factor regarding the violation of the right to privacy. In the case of the right to be forgotten, it is a question of whether the damage was caused by the search results. So, in the case of *Tamiz v. the United Kingdom* the Court ruled that the Google blog publishing service is not responsible for comments, since the damage caused by such comments did not

[292] ECtHR: Judgment of 28 September 2018, *M.L. and W.W. v. Germany*, App nos. 60798/10 and 65599/10.

exceed the level of trivial effect.[293] In other words, the ECtHR ruled that the damage in this case was not significant. In *Einarsson v. Iceland*, the Court found that posting a photo on Instagram violated the right to respect for privacy, since a message posted on a publicly accessible website could reach a large number of people. That is, the Court took into account the number of people who had access to this piece of content when assessing the severity of the damage. On the contrary, in the *Google Spain* case, the CJEU suggested that a violation of an individual's rights could be established even if the individual concerned had not suffered any damage.

In addition, the ECtHR considers the position of search engines only in passing, limiting itself to the statement that due to their reinforcing effect on the dissemination of information, the obligations of search engines to a person claiming the right to be forgotten may differ from the obligations of the original publisher of information.

[293] ECtHR: Judgment of 19 September 2017, *Tamiz v. the United Kingdom*, App no. 3877/14.

6 The right to be forgotten: challanges and perspectives for EU data protection law

6.1 Right to be forgotten as a mechanism for the provision of personal identity

The development of information technology has led to the emergence of a "digital person", according to R. Clark, D. J. Solove and L. Floridi.[294] With the help of these technologies, a person's identity is "assembled" from his "digital parts". Moreover, the formula "one person - one identity" no longer reflects reality, as personal identity becomes dispersed, multiple, ubiquitous, decentralized and eternal.[295]

The advent of the Internet of Things (IoT) and the Internet of Body (IoB) are changing and expanding the ways and tools of expressing, representing and projecting a person's identity from third parties, especially for marketing, which is typical for business on the Internet. Moreover, the creation of a digital profile of a person is practically independent of his actions or consent. In conditions of non-transparency of data processing, the unlimited possibility of obtaining such data using the "myth of consent" means consent to profiling, on the one hand, and consent to fragmentation of the digital self, on the other hand. Getting out of control and the sphere of human control, the elements of his/her identity become an object of appropriation, falsification, making a person more vulnerable. P. De Hert analyses the need to recognize the "right to identity" in the light of the threats posed to humans by the Internet of Things (IoT), defining profiling as the most important threat to identity, which creates new opportunities for manipulating people.[296]

At the same time, the same information technologies have given the person himself the opportunity to project his identity in the digital space, for example, through the right to be forgotten. As N. Andrade notes: "The proposed conceptualization of the right to be forgotten

---

[294] FLORIDI, Luciano. The Information Society and Its Philosophy: Introduction to the Special Issue on The Philosophy of Information, Its Nature, and Future Developments. *The Information Society*, Vol. 25, No. 3, 2009, pp. 153–158; CLARKE, Roger. The Digital Persona and Its Application to Data Surveillance. *The Information Society*, Vol. 10, No. 2, 1994, pp. 77–92; SOLOVE, Daniel J. The Digital Person: Technology and Privacy in the Information Age. *New York University Press*, 2004, 296 p.

[295] ANDRADE, Norberto Nuno Gomes de. Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization. In GUTWIRTH, Serge, et. al. (eds.). *Computers, Privacy and Data Protection: An Element of Choice*. Springer, 2011, pp. 65-97.

[296] DE HERT, Paul. A right to identity to face the Internet of Things. Council of Europe Publishing [online]. 2007. [cit. on. 25th December, 2023]. Accessible at: <https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf>.

not only makes sense from an identity point of view, it also contributes to the further development of the modern conception of identity, reinforcing its 'anti-essentialistic' understanding".[297] Such a projection involves the creation of self-images in the digital space that reveal the elements of a person's personality. With the creation of these self-images, a person's digital life enters into another aspect of human existence, which, although closely related to traditional life, is nevertheless characterized by specific interactions with other people. Providing legal protection only to personal data, regardless of the protection of the individual himself, is erroneous: the personal data that make up a person's digital life are not just data — they are the constituent elements of a digital personality. "All data about us, in fact, are components of our personality", - notes R. Richterich. [298]

The life of a modern person gets another dimension - digital. It is impossible to legally protect one dimension and ignore the other. The new dimension increases the pressure on the law, as the massive exchange of personal information that has occurred with the widespread adoption of the platform, along with the "communication power", has made people more vulnerable.[299] I believe that the existence of a digital person and digital life presupposes the expansion of the legal coordinates of the individual and reveals the need to develop more comprehensive mechanisms for protecting the individual in the digital world.

Creating or choosing your own content for your digital identity involves providing a person with the legal tools with which they create and protect their choice. To paraphrase Benn, who points out that if an individual is confident that he/she can be himself/herself, he/she can believe in himself as a person,[300] It can be said that the law should provide a person with confidence that he/she can be the person he/she wants to be. In this sense, a person is a subject who realizes himself/herself as an agent choosing and trying to control his/her own course in the digital world. The new, informational nature of identity makes it a matter of data processing and information management, therefore many legal mechanisms that are provided and applied in the context of personal data protection can become legal tools for identity protection. Thus, G. Pino, characterizing the right to personal identity as a fairly flexible right, considers it closely

---

[297] ANDRADE, Norberto Nuno Gomes de. Oblivion: The Right to Be Different from Oneself - Reproposing the Right to Be Forgotten. *Revista de Internet, Derecho y Política*. No. 13, pp. 122-137.

[298] RICHTERICH, Rachel. L'intégrité numérique: le vrai combat pour nos données. LeTemps, [online]. 11 January 2019. [cit. on 25th December 2023]. Accessible at: < https://www.letemps.ch/profil/rachel-richterich?before=2019-01-29T11%3A28%3A00%2B01%3A00>.

[299] VARDANYAN, Lusine, et. al. Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. *TalTech Journal of European Studies*, Vol.12, No.1, 2022, pp.159-185.

[300] BENN, Stanley I. Privacy, freedom, and respect for persons. In SCHOEMAN, Ferdinand David (ed.) Philosophical Dimensions of Privacy: An Anthology, Cambridge: Cambridge University Press, 1st edition, pp. 223–244.

related to the right to be forgotten and the right to personal data protection.[301] As E. Oreg notes, the broad definition of "processing" and "personal data" in the GDPR covers cases of identity violation.[302] Nevertheless, the modern paradigm of personal data protection cannot fully ensure the right to identity in the digital world, and that is why.

As already noted, the GDPR accepts the general concept of personal data, but does not protect the internal relationship between personal data and identity. As Urgessa notes: "the existing data protection regime in the EU protects information that relates to us but does not, strictly speaking, protect us". [303]

The philosophy points to the existence of the *idem* and *ipse* identities. '[T]he idem identity corresponds to a view on the individual from the outside, which treats the individual as a sum of stable characteristics. The ipse identity [...] corresponds to the individual as he or she relates to him/herself".[304] The GPDR regulates the use of *idem* identity elements, a set of characteristics that make it possible to identify a person.

Therefore, it can be said that this right provides an autonomous mode of using "personal data" without communicating with a person. In turn, the GDPR rather regulates the use of identity elements – a subjective dimension of a person, including his habits or preferences, for which data is often processed. In other words, the GDPR does not proceed from the fact that personal data (or part of it) is a projection of personality. Meanwhile, this type of personal data is a component of personal identity because there is no difference between the information sphere of a person interpreted by this internally personal data and their personal identity.[305] At the same time, the use of this data as a kind of projection of personality requires stronger and more fundamental protection than can be achieved within the framework of the right to personal data protection. The current legal protection of information identity is insufficient and does not cover a wide range of personal hazards.

For such fundamental protection, the doctrine proposes to justify the protection of personal data through the right to personal identity. Thus, N. Andrade considers the right to

---

[301] PINO, Giorgio. l'identità personale. In RODOTÀ, Stefano, TALLACCHINI, Mariachiara (eds.), Trattato di biodiritto, 2010, vol. I, Ambito e fonti del biodiritto. Milano: Giuffrè, 297-321 p.; See also PINO, Giorgio. Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali. In PANETTA, Rocco (ed). Libera circolazione e protezione dei dati personali, 2006, MILANO: Giuffre', 275-321 p.

[302] OREG, Elad. Right to Information Identity, *John Marshall Journal of Computer & Information Law*, 2012, Vol. 29., No. 4, pp. 539-592.

[303] URGESSA, Worku Gedefa. *The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging 'Data' as Exclusively Informational,* JIPITEC, Vol. 96, No. 7, 2016, p. 1.

[304] KHATCHATOUROV, Armen. Digital Regimes of Identity Management: From the Exercise of Privacy to Modulation of the Self. In KHATCHATOUROV, Armen. et al. (eds.). Digital Identities in Tension: Between Autonomy and Control, London: ISTE Editions, 2019, p. 30.

[305] FLORIDI, Luciano. The ontological interpretation of informational privacy. Ethics and Information Technology, 2005, Vol. 7, No. 4, pp. 185-200.

personal identity as a right that covers, controls and protects a number of different types of information related to our personal identity or its component (digital, genetic, neural). N. Andrade defines the right to personal identity as the right to be different, unique and unique. The right to identity is presented and developed as a right that regulates a series of movements and transformations of identity between different ontological levels of "being" (possible ↔ real; actual ↔ virtual). Thus, the right to identity is the right to register the attributes of one's identity (real → possible), as well as the right to recognition and identification (possible → real) in accordance with these defining features. The right to identity also includes the right to be presented the way you want (virtual → actual), that is, the right not to be misrepresented; the right to delete and recreate oneself (actual → virtual), the identity movement, which includes the right to be forgotten (and, therefore, the right to start anew) and the right to multiple identities (virtual → real) – that is, the right to create, control and maintain different identities in a digital environment.[306]

P. Bernal includes three groups of rights as components of the "right to online identity": the right to create, assert and protect this identity, as well as the right to control the connections between online identity and the real person behind it.[307] The author argues that the rights that form the right to identity should function as principles from which legal rights and rules can then be derived. P. Bernal, like N. Andrade, argues that the right to be forgotten can directly flow from the right to online identity. In this understanding, the right gives the opportunity to choose the information, the data as the "building blocks" that will form his/her digital identity, the choice of "which information about him is and will be available and accessible", [308] as well as to maintain and control what will be his/her reputation and dignity (even after death, what will be discussed in the next paragraph). From the above-mentioned point of view, the right of each person to create their own digital identity perimeter may become a new perspective on the recognition of the right to digital identity as the basis for information self-determination. As you know, the GDPR states that individuals should have control over their personal data, and lays the foundation for recognizing the right to information self-determination, the content of which can be determined using GDPR rights, i.e. the rights to receive information, delete, correct, access, object, restrict processing, data portability and not be subject to a decision based

[306] DE ANDRADE, Norberto Nuno Gomes. *The right to personal identity in the information age: a reappraisal of a lost right*. Florence: European University Institute, 2012, Ph.D. Thesis, Italy.
[307] BERNAL, Paul A. The Right to Online Identity. SSRN Electronic Journal [online]. September 2012. [cit. on 25th December 2023].
Accessible at: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143138 >.
[308] VARDANYAN, Lusine, et. al. Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. *TalTech Journal of European Studies*, Vol.12, No.1, 2022, pp.159-185.

solely on automated processing. I believe that recognizing the digital identity of an individual as a fundamental right will mean laying a new foundation for the rights provided for in the GDPR.

Moreover, even in its case law, the CJEU reflects on the right to be forgotten as a certain emphasis on the assumption of the possibility of "managing" a digital person. In particular, in the *Google Spain* judgment, a person is granted the right to withdraw a link from search engines. As one can see, this judgment gives a person a tool that allows them to control their digital identity. Thus, everyone can simulate their projection in the digital world by requesting the removal of a search engine index that is considered inadequate. Thus, the right to be forgotten becomes one of the tools for the formation of digital identity as the basis for information self-determination. I would like to note that considering the right to be forgotten in this way can expand the scope of its application, become a so-called paradigmatic shift from the justification of confidentiality to the justification of identity.

The transition of consideration of the right to be forgotten from the justification of privacy to the justification of identity can significantly strengthen human protection in the digital world. First of all, this concerns improving efficiency in balancing the right to be forgotten with the right to express opinions and access to information. As C. Sullivan points out, unlike the right to privacy, deviations from the right to identity cannot be justified by considerations of public interest and can only take place in exceptional circumstances, therefore the right to identity provides better protection than the right to privacy.[309] P. De Hert emphasizes the need to clearly distinguish the right to identity from the right to privacy. P. De Hert identifies specific issues related to identity that are not covered and are not protected by the right to privacy, among which is the recognition of the right to be forgotten. The author argues that these new developments can have an important impact on our understanding of identity and require a new balance of interests that requires going beyond established rights and concepts such as privacy, freedom, autonomy and discrimination.[310] I agree with the author, since the right to privacy protects personal information that is in the private sphere. It provides protection against the publication of this information and its withdrawal from personal life. At the same time, the right to be forgotten (the right to be forgotten) is aimed at protecting against the dissemination of already published information, which, due to certain circumstances,

[309] SULLIVAN, Clare. Digital Identity – the Legal Person? *Computer Law and Security Review* Vol. 25, No. 3, 2009, pp. 227-236.
[310] DE HERT, Paul. A right to identity to face the Internet of Things. *Unesco*. [online]. 2007, Accessible at:<https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf>.

distorts the modern idea of a person, his current identity. Consequently, the expansion of the context of the right to identity strengthens the application of the right to be forgotten.

In addition, a lot of personal data is contained in publications on social networks or on platforms such as YouTube. Such information is protected by the fact that it is processed exclusively for "journalistic purposes" and does not fall within the scope of the GDPR. The GDPR restricts the right to be forgotten in cases where restrictions are permissible for "journalistic, artistic or literary expression, to protect public interests in the field of public health, or for historical, statistical or scientific research purposes." However, if I consider the right to be forgotten in the context of the right to identity, such an exception may not work. If information can create a misconception about a person's personality, that is, a discrepancy between the personality transmitted through outdated information and the one that the individual wants to represent now, there is a possibility of applying the right to be forgotten.
The right to be forgotten can be considered as a mechanism for the formation and choice of identity, which is dynamic and which can be constantly revised, due to its conditionality with the level of human development and over time. The ECtHR deduces the right to identity from the interpretation of Article 8 of the ECHR. In the case of *Tysiąc v Poland*, the ECtHR has confirmed that "private life" is a broad term covering, among other things, aspects of physical and social identity, including the right to personal autonomy, personal development, as well as to establish and develop relationships with other people and the outside world. Moreover, the ECHR emphasises not only the negative, but also the positive aspect of the right to respect for private life, in particular through the inclusion of the right to develop one's personality within the framework of the right in question: such a personality develops not only "by itself", but also in our relations with other people and the outside world.[311] According to C. Sullivan, the ECtHR's position on personal identity is based on understanding the latter as a narrative, a continuous process of creating and recreating the story of one's own life.[312] Tirosh argues, the right is neither an infringement of the right to free expression nor a guarantee for privacy but rather the right to construct one's own narrative, appealing to the fact that people are given more of a 'control-right' over their own personal data and therefore their identity.[313]

---

[311] MARSHALL, Jill. Personal Freedom through Human Rights Law?: Autonomy, Identity and Integrity under the European Convention on Human Rights, International Studies in Human Rights, Boston: Martinus Nijhoff Publishers, Vol. 98. 2009,
[312] SULLIVAN, Clare, Privacy or Identity? *International Journal of Intellectual Property Management* Vol. 2, no. No. 3, 2008, p. 297.
[313] TIROSH, Noam. 'Reconsidering the "Right to Be Forgotten' – Memory Rights and the Right to Memory in the New Media Era. *Media, Culture & Society*, 2017, Vol. 39, No. 5, p. 645.

The right to be forgotten can turn into the right to represent an actual personal identity, who a person is and who they want to represent in society. Determining the details of one's physical and social identity contributes to personal development, since an individual has the right to such information, and this is important because of its influence on personality formation. Thus, our democratic society must ensure that we can participate in shaping our future identity, as well as be able to remove certain parts of our past. This emphasises respect for the free choice of information by each individual.

As Andrade points out, since a valid identity can prevail only when past identities are forgotten, the right to be forgotten can play an extremely important role, allowing an individual to reconstruct the narrative of identity with confidence that past identities will not undermine this process.[314]

Thus, modern threats to the individual in the digital world cannot be levelled through the application of a modern legislative framework in the context of the right to privacy. The right to be forgotten is closely related to the ability to rethink oneself, form one's identity and present one's actual identity to the world. From the point of view of ipse identity, the mechanisms specified in the GDPR cannot be considered effective since they do not help a person present himself to others as a person wants, however, the right to be forgotten has the potential to become mechanisms for protecting such identity. Considering the right to be forgotten in the key of personal identity may help to find a new balance of interests.

6.2 Post-mortem privacy and the right to be forgotten

The studies inherent to data "perpetuity"[315] have focused on governing data related to living individuals, mostly in line with the right to be forgotten.[316] The debate surrounding the legal regime of personal data is currently also involving the post-mortem time. E. Bourdeloie writes that people leave digital footprints throughout their lives, after the death of a person, the preservation of this information contributes to the "survival of the digital personality of the deceased".[317] The disconnection between an individual's biological existence and his/her electronic counterpart

[314] ANDRADE, Norberto Nuno Gomes de. Oblivion: The Right to Be Different from Oneself - Reproposing the Right to Be Forgotten. *Revista de Internet, Derecho y Política*. No. 13, pp. 122-137.
[315] RESTA, Giorgio. La "morte" digitale. Milano: Giuffrè Editore, 2014, 892 p.
[316] Among the many scholars who have been dealing with the topic, see FINOCCHIARO, Giusella. Il diritto all'oblio nel quadro dei diritti della personalità. Il Diritto Dell'informazione e Dell'informatica, Vol. 4 No. 5, 2014, pp. 591-604; ROSEN, Jeffrey. The right to be forgotten. Stanford Law Review Online, 2012, Vol. 64, pp. 88–92.
[317] BOURDELOIE, Hélène. Usages des dispositifs socionumériques et communication avec les morts. Questions de communication. Vol. 28, 2015, p. 103.

leads to the fact that the locus of digital presence is no longer limited by physical attributes. This reflects one of the modern anthropological gaps associated with the human body, which until now has been perceived as a "receptacle" of personality identity. Nowadays, in the context of the digital world, personal data itself has become such a "container". The biological body may no longer exist, but feelings, consciousness, actions and will have already passed, exist and will constantly exist in the digital world as expressions of human identity. As the shift to the digital continues, careful stewardship of digital content, which can, in some sense, be said to be a rich reflection of you, is more and more necessary, [318] including after death.

However, within the existing legal framework, this will be a very difficult task. GDPR has left the issue of posthumous protection of personal data without due attention. According to Recital 27 of the GDPR: "This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons".[319] The GDPR thereby leaves the issue of posthumous protection of personal data at the discretion of the EU Member States. Moreover, the GDPR does not oblige EU Member States to provide in their legislation special rules for the processing and protection of personal data of the deceased. This EU policy has led to the fact that some EU Member States, such as Germany, Ireland or Cyprus, have not provided in their legislation any special rules for the processing and protection of personal data of the deceased, but others, such as, for example, Sweden,[320] explicitly exclude this protection. Despite the fact that the EU Charter in Article 8(1) provides that "Everyone has the right to protection of personal data concerning him or her", nevertheless, there is no direct assumption of protection of posthumous rights. Although, to be fair, it should be noted that in the *Lindqvist* case, the CJEU indicated that "(...) nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof, provided that no other provision of Community law precludes it".[321] This indirectly allows only the possibility of posthumous data protection, leaving it to the discretion of the EU Member States. However, the digital network, which is a global network, requires more comprehensive regulation of this area.

---

[318] CARROLL, Evan, ROMANO, John. *Your digital afterlife: When Facebook, Flickr and Twitter are your estate, what's your Legacy?* Berkeley, CA: New Riders, 2011, 203 p.

[319] See Recital 27 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement ofsuch data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[320] See Section 3 of the Swedish Personal Data Protection Act (Sw. Personuppgiftslag (1998:2014)).

[321] Court of Justice of the European Union: Judgment of the Court of 6 November 2003, *Criminal proceedings against Bodil Lindqvist.* C-101/01, para. 98.

The ECtHR also takes a cautious approach in its practice. So, in the cases of *Yakovlevich Dzhugashvili v. Russia*[322], *Koch v. Germany*[323], *Sanles Sanles v. Spain*[324] or *Thevenon v. France*[325] the Court ruled that Article 8 of the Convention should apply only to a living person, but not to a deceased one, since it is "non-transferable". In the case of the property of *Estate of Kresten Fittenborg Mortensen v. Denmark*, the Court stated that, despite the fact that "the concept of "private life" is a broad term not susceptible to exhaustive definition"[326] which "covers the physical and psychological integrity of a person"[327] and "a compulsory medical intervention, even if it is of minor importance, it constitutes an interference with the right to respect for a person's private life",[328] " however, it would stretch the reasoning developed in this case-law too far to hold in a case like the present one that DNA testing on a corpse constituted interference with Article 8 rights of the deceased's estate ".[329] At the same time, in cases such as *Jäggi v. Switzerland*, the Court recognized, that "right of the deceased, deriving from human dignity, to protect their remains from interferences contrary to morality and custom".[330] In the case of *Genner v. Austria*[331] the Court took a more ambiguous approach, confirming that "to express insult on the day after the death of the insulted person contradicts elementary decency and respect for human beings […] and is an attack on the core of personality rights.". [332]

In the case of *M.L. v. Slovakia*, the Court considered a specific aspect of the right to be forgotten – realization in the event of the death of an interested party.[333] M.L. was the mother of a priest who was convicted of sexual abuse of a minor and hooliganism and who died after serving a criminal sentence. Three newspapers published articles suggesting that the cause of the priest's death could be his previous criminal convictions. M.L. began legal proceedings against the publishers, claiming that this information was unfounded and violated her rights and the privacy rights of her late son. The court considered the case and found it admissible, taking into account the violation of both the rights of M.L. and the deceased relative. The Court recognized that

---

[322] ECtHR: Judgment of 9 December 2014, *Yakovlevich Dzhugashvili v. Russia*, App. no. 41123/10, para. 23-24.
[323] ECtHR: Judgment of 17 December 2012, *Koch v Germany*, App. no. 497/09, para 78.
[324] ECtHR: Judgment of *Sanles Sanles v. Spain*, no. 48335/99, ECHR 2000-XI.
[325] ECtHR: Judgment of 28 June 2006, *Thevenon v. France*, App. no. 2476/02.
[326] ECtHR: Judgment of 12 January 2010, *Gillan v. Quinton v the United Kingdom*, App. no. 4158/05, para 61.
[327] Ibid.
[328] ECtHR: Judgment of 13 December 1979, *X v. Austria*, App. no. 8278/78, para. 155; ECtHR: Judgment of 10 December 1984, *Acmanne and Others v. Belgium*, App. no. 10435/83, para. 254.
[329] ECtHR: Judgment of 15 May 2006. *The Estate Of Kresten Filtenborg Mortensen v. Denmark*, App. no. 1338/03.
[330] ECtHR: Judgment of 13 July 2006. *Jäggi v. Switzerland*, App. no. 58757/00.
[331] ECtHR: Judgment of 12 January 2016. *Genner v. Austria*, App. no. 55495/08.
[332] MALGIERI, Gianclaudio. *R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions*. In LEENES, Ronald et. al (eds.). *Data Protection and Privacy: The Internet of Bodies*. 2018, Hart Publishing, pp. 300-320.
[333] ECtHR: Judgment of 14 October 2021, *M.L. v. Slovakia*, App. no. 34159/17.

Article 8 of the Convention also covers cases where a person treats the deceased out of respect for the feelings of the deceased's relatives.[334] The Court considered in the traditional way the case of the conflict between freedom of expression and protection of privacy. However, these criteria had to be applied to information that related to the deceased person and could affect the private sphere of a relative. In fact, the Court argues that the right to oblivion may extend to a deceased person with the possibility of its exercise also by a relative. Prior to that, the Court accepted claims for violation of privacy protection only if the insult to the reputation of the deceased person affected the applicant's private life. However, the inconsistency of judicial practice in this matter does not yet make it possible to unequivocally conclude that the right to be forgotten is allowed for the deceased person.

Nevertheless, the approach of the EU legislator is theoretically connected with the assumption that the deceased cannot have or exercise personal rights is already being questioned today. Thus, the dissenting opinion of the ECHR judge Fura-Sandstrom in the case of *Akpinar-Altun v. Turkey* in this aspect is very significant.[335] The judge pointed out that it is the responsibility of the State to respect the dignity of the individual and protect physical integrity cannot be considered to cease with the death of the person in question.[336]

It seems to me that the approach that is generally accepted in EU law is no longer correct in light of the development of a networked society and the phenomenological gap between online and offline human presence justifies efforts to solve problems of legal qualification of tools and remedies that can be applied to ensure effective posthumous protection of human rights in the digital sphere, including the right to be forgotten. This is especially important because due to the lack of a legal framework, the issue is left to the unlimited discretion of the Internet service providers and social media companies themselves, which provide a postmortem data protection policy that is convenient for them. Often, such policies are often not formalized in the general terms and conditions. For example, Facebook's legacy contact policy allows account users to turn a deceased person's account into a memorial.[337] OkCupid has a policy according to which a service user's subscription for the Service will continue indefinitely until cancelled by the user.[338] However, practice shows that this creates obstacles for the removal of the deceased's account by relatives. Referring to the case of Justin M. Ellsworth and Yahoo! J.C. Buitelaar correctly points

---

[334] See Ibid, para. 23.
[335] Article 2-terdecies, of the Italian Legislative Decree 196/2003, introduced by Article 2, paragraph 1, letter f, of the Legislative Decree n. 101/2018.
[336] Article 40-1. The French Data Protection Act No. 2018-493 of 20 June 2018.
[337] Facebook Help Centre: What is a legacy contact and what can they do? [online]. Accessible at: <https://www.facebook.com/help/1568013990080948>.
[338] OkCupid's Terms and Conditions. [online]. Accessible at: <https://www.okcupid.com/legal/terms>.

out that: "when the Internet user wishes to assume the role of a responsible steward, they find Internet providers barring the way. It is curious to note these providers pretend to do so exactly for the sake of protecting the privacy of their user".[339] Some providers even claim ownership of their customers' email accounts under the pretext that this is necessary to protect user privacy.[340]

6.2.1 Discussion of the issue of post-mortem data protection in the doctrine

There is also no developed unified approach in the legal literature on how to solve legal issues of posthumous protection of personal data within the EU. As a possible solution to the issues of posthumous data protection, G. Malgieri sees a combination of posthumous privacy and quasi-ownership of the heirs to the "digital body" of the deceased person.[341] L. Edwards and E. Harbinja advocate recognition of posthumous right to privacy.[342] They base this view on the dignity of a deceased person, which deserves protection not only in the physical world, but also in the digital one. B. Zhao believes that the heirs of a deceased person have two posthumous interests, namely reputation and privacy,[343] and both of them are unequivocally recognized by EU law. E.L. Okoro argues that there is no need for posthumous data protection at the level of EU legislation: "At European Union level, a call for posthumous personal data will not be welcomed and answered by all Member States as each state has its own unique history and traditional beliefs upon which its legal system is built".[344] V. Mayer-Schoenberger supports the policy of deleting personal data of deceased Internet users after their death.[345] However, I do not see this as a good solution to the problem, because according to this approach, personal data containing information about a person's contribution to history, science or art should also be deleted. In addition, it casts doubt on the possibility of the existence of mechanisms to protect digital identity.

---

[339] BUITELAAR, Jan. Post-mortem privacy and informational self-determination.Ethics and Information Technology, Vol. 19, No. 2, 2017, pp. 129-142.
[340] ATWATER, Justin. Who owns E-mail? Do you have the right to decide the disposition of your private digital life? *Utah Law Review*. 2006. Vol. 2006, No. 2, pp. 397-418.
[341] See MALGIERI, Gianclaudio. *'R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions'*. In LEENES, Ronald et. al (eds.). *Data Protection and Privacy: The Internet of Bodies*. 2018, Hart Publishing, pp. 300-320.
[342] EDWARDS, Lilian, HARBINJA, Edina, Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World. *Cardozo Arts & Entertainment Law Journal*, Vol. 32, No. 1, 2013, pp. 83-129.
[343] ZHAO, Bo. Posthumous Defamation and Posthumous Privacy Cases in the Digital Age. *Savannah Law Review*, Vol. 3, No. 1, 2016, pp. 15-35.
[344] OKORO, Egoyibo Lorrita. Death and Personal Data in the Age of Social Media. Tilburg: Tilburg University. LLM Law and Technology, 2018, 48 p.
[345] MAYER-SCHÖNBERGER, Viktor. Delete: The virtue of forgetting in the digital age. Princeton: Princeton University Press, 2009, 272 p.

One of the arguments pointed out by opponents of the right to posthumous privacy is that violations of the right to privacy do not harm the deceased. They consider the violation of the privacy of the deceased as "no-effect injury", taking into account the fact that the deceased is unable to protect his/her personal data or realize his/her digital identity.[346] However, as J. Feinberg notes, the principle of harm also covers retroactive harm, which is caused not only to a posthumous person as a result of events that occurred after his death, but also as a result of substitute or posthumous events that harm his remaining digital counterpart, even if he does not know about it.[347] It is also possible to apply the principle of harm to a digital person if a person is understood as "our abilities to believe, learn, and feel, and so on, (…) including that which is said, thought, and written about the person — subsisting in the speech and memory of living persons as well as in information held in impersonal media".[348] As S. Winter writes: "During my life, the various aspects of my personhood form a (more or less) cohesive and interactive whole and the status of my reputation (my public persona) matters to me regardless of what I know concerning changes to it".[349] In the sense of the application of the right to be forgotten, the EU case law is generally not conditioned by the presence or absence of damage to the data subject. It seems that the main purpose of the right to be forgotten is still to guarantee "the right not to be a victim of harm." In addition, even if the deceased is unable to protect his personal data, this does not mean that the harm "has no consequences". Firstly, one should not forget about living relatives: in any case, such a violation causes direct harm to their reputation and interests. The privacy and reputation of the deceased become an integral part of the reputation of his relatives, regardless of their desire to be protected. Secondly, as K.R. Smolensky rightly points out: "Assume that a person dies and their neighbour spreads defamatory remarks about them. These remarks hurt the decedent's reputation, regardless of whether they are alive and can become emotionally upset by the statements. The fact that they do not know about the harm does not mean that a harm to the decedent's interest, namely their reputation, has not occurred".[350]

E. Oreg, speaking for the recognition of the new legal principle of the "right to information identity" understands this principle as human rights to the functionality of

---

[346] WINTER, Stephen. Against posthumous rights. *Journal of Applied Philosophy*, 2010, Vol. 27, No. 2, pp. 186-199; See also FLORIDI, Luciano. The informational nature of personal identity. *Minds and Machines*, 2011, Vol. 21, No. 4, pp. 549-566.

[347] FEINBERG, Joel. The moral limits of the criminal law: volume 3: harm to self. Oxford University Press, 1989, 448 p.

[348] WINTER, Stephen. Against posthumous rights. *Journal of Applied Philosophy*, 2010, Vol. 27, No. 2, pp. 186-199.

[349] Ibid.

[350] SMOLENSKY, Kirsten Rabe. Rights of the dead. *Hofstra Law Review*. 2009, Vol. 37, No. 3, pp. 763-803.

information platforms that allow others to identify and recognize him, as well as remember who and what he is.[351] It is in the context of memory that qualitative changes occur in the information society: if human memory naturally tends to forget certain facts over time, evolve, and change meaningfully, then digital memory does not allow for change and the memory of a person remains constant and frozen in time.

According to S. Rodota, with the creation of increasingly large databases available on the Internet through search engines, social memory is expanding and conditioning individual memory. If there used to be a *damnatio memoriae*, now there is a duty to remember, since the collective memory of the Internet accumulates all traces of people's lives, making them prisoners of the past, challenging the formation of a free personality. This leads to the need for adequate remedies, such as the right to be forgotten to protect the privacy and freedom of the individual.[352] To J.E. Rhea's statement that the effect of the eternity of memory raises the question of oblivion as a philosophical and psychological problem,[353] one can also add legal questions.

Eternal memory in the truest sense of the word, however, does not exclude the fact that the personal data of the deceased, which are freely available on the Internet, cannot lose their social significance in the process of changing life circumstances, or contain incomplete, inaccurate, unreliable or reliable, but defamatory or offensive information. In this case, if the publication and disclosure of such information on the Internet occurred in an EU member state whose legislation does not contain special rules for the processing and protection of personal data posthumously, the memory of a person and his information identity will be distorted and violated. D. Sperling correctly notes that: "(…) even though a person may not survive their death, some of their interests do".[354] A similar approach is followed by K. Smolensky, who is inclined to believe that: "While it is true that only a subset of interests may survive death, and even a smaller subset receives legal protection, death does not necessarily cut off all interests, and consequently, it does not end all legal rights. Recognition of posthumous legal rights gives the dead a significant moral standing within our legal system, as would be expected if lawmakers are driven by the desire to treat the dead with dignity".[355] The justification of the right to be forgotten

---

[351] OREG, Elad. Right to Information Identity, *John Marshall Journal of Computer & Information Law*, 2012, Vol. 29., No. 4, pp. 539-592.
[352] RODOTÀ, Stefano. Dai Ricordi Ai Dati L' Oblio È Un Diritto?. *La Reppublica.it* [online]. 30th January 2012. [cit. on 25th December 2023]. Accessible at: <https://ricerca.repubblica.it/repubblica/archivio/repubblica/2012/01/30/dai-ricordi-ai-dati-oblio-un.html>.
[353] RHÉA, Eddé. Le droit: un outil de régulation du cyberespace? Le cas du droit à l'oubli numérique. *L'Homme & la Société*. 2018, Vol. 1, No. 206, p. 69.
[354] SPERLING, Daniel. Posthumous Interests. Cambridge: Cambridge University Press, 2008, 304 p.
[355] SMOLENSKY, Kirsten Rabe. Rights of the dead. *Hofstra Law Review*. 2009, Vol. 37, No. 3, pp. 763-803.

through the protection of human dignity allows us to get out of the situation of the "impossibility" of the right to be forgotten, because the broad concept of human dignity can offer protection not only of the deceased person, but also of his/her remains.

The concept of the right to be forgotten through the protection of human dignity reveals important aspects that go beyond simple "oblivion" in the digital age. It involves protecting not only a person during his life, but also after death, covering both his/her digital heritage and the remnants of his/her personality in the digital space. The idea of preserving the dignity of a person after his departure is reflected in the understanding of the concept of "digital remains". They are an integral part of our digital lives, representing aspects of personality that continue to exist even after a person leaves. In this context, the attitude towards "digital remains" requires respect and protection, like respect for the person himself for his/her dignity.

The right to be forgotten, formulated through the prism of the right to dignity, suggests the idea of posthumous privacy. This means that information about a person after they leave must be protected and should not be used or distributed without appropriate consent. Considering dignity in the Kantian sense, this assumes that human dignity is present even after death, and its preservation includes the protection of both the memory of a person and his digital traces.

The principle of preserving human dignity is present in Article 1 of the Universal Declaration of Human Rights and in Article 1 of the CFR. A. Cayol believes that the memory of the dead can be protected on the basis of respect for human dignity.[356] The memory of the departed can be protected on the basis of respect for their human dignity, which forms the basis for the protection of their digital remains and information about them. Thus, the application of the right to be forgotten in the context of human dignity implies broader protection not only of the individual during life, but also the preservation of his/her integrity after leaving this world. This calls for an ethical approach to the treatment of digital heritage based on respect for the inviolability of the human person and his dignity, which remains after death.

As noted earlier, the legal practice of the ECtHR confirms that "private life" covers, among other things, aspects of physical and social identity, including the right to personal autonomy, personal development, as well as to establish and develop relationships with other people and the outside world,[357] The ECHR emphasizes the positive aspect of the right to respect for private life, in particular through the inclusion of the right to develop one's personality within the framework of the right in question, thereby understanding personal

[356] CAYOL, Amandine. Avant La Naissance et Après La Mort: L'être Humain, Une Chose Digne de Respect. *Cahiers de La Recherche Sur Les Droits Fondamentaux*, No. 9, 2011, p. 124

[357] ECtHR: Judgment of Grand Chamber of 4th December 2008. *S. and Marper v. The United Kingdom*. Nos. 30562/04 and 30566/04.

identity as a continuous narrative of one's own life story, which no longer ends with biological death - the latter becomes just another event in the narrative. Normative, informational activity allows a self-governing individual to declare himself/herself as a person and constantly and implicitly present his life story in ongoing autobiographical narratives, thereby ensuring the posthumous and proper continuation of his life's work.[358] Our public persona, both during life and after death, is preserved in speech, memory and information stored in public media comparable to autobiographies. It is the textual ontology of personality that persists after death. With the advent of the Internet, the human narrative becomes continuous, which gives rise to the expansion of the right to protect the digital personality after death, including through the application of the right to be forgotten, which in this case becomes a tool for protecting dignity. In the post-mortem period, this right will make it possible not only to preserve the projected identity in the context of one's narrative, but also in limited cases to correct it.

Why do we need the possibility of correction? First of all, because the Internet not only makes it possible to tell and preserve one's own narrative, but also limits this possibility at the same time. With the democratization of data collection methods, virtually everyone has the ability to gather information about others, profiling and predicting often with algorithms thereby shaping even a person's future narrative. Additionally, data-driven companies have more information about the average person than the average person themselves, and the latter may be in a better position to write a personal narrative than we are ourselves, as we will never have access to some of our own data. The ability to participate in the narrative itself and identity formation is undermined. Moreover, algorithmic digital identification creates a partial and distorted representation of the person and the use of digital data to create an image of a deceased person can thus lead to a distortion of the person's identity, image and memory. Therefore, protecting the digital identities of social media users from distorted information remains relevant even when life ends.

The existence of the digital person and digital life implies the expansion of the legal coordinates of the personality and reveals the need to develop more comprehensive mechanisms for the protection of the personality in the digital world. Creating or choosing one's own content for one's digital identity implies providing the individual with the legal tools by which he or she is provided with such protection for his or her choices. The posthumous exercise of personal data rights, including the right to be forgotten, represents a possible answer to the legal

[358] BUITELAAR, Marjo 'Discovering a different me': Discursive positioning in life story telling over time. *Women's Studies International Forum*, 2014. Vol. 43, pp. 30-37.

questions raised by new technologies regarding the fate of digital assets after the death of the data subject.

The right to be forgotten acts as an essential counterweight to digital memory.[359] Since people now have the opportunity to intervene in the future using their digital data, it is obvious that the simplest solution is that they will automatically provide the opportunity to anticipate this situation. From a general point of view, we are talking about the transition to a new control over the use of data, that is, a more active and less passive attitude to their protection in the digital world.[360] Staying in the logic of memorization and constant accumulation of information can violate the reputation, dignity, inviolability of the individual, and desecrate his/her memory after death.

6.3 "Streisand effect": unwanted paradoxes of right to be forgotten

6.3.1 How does the CJEU inadvertently protect the "right to be remembered"?

The EU is trying to strengthen its position in the digital world as a guarantor of the rights of its own citizens, and the right to be forgotten thereby becomes one of the foundations for the formation and development of its digital sovereignty.[361] However, despite the fact that the CJEU itself, through its own case law, gradually draws the contours of the right to be forgotten, nevertheless, it itself turns this right into an instrument unsuitable for the protection of human privacy in the digital world. The problem lies in the very wording that the Court uses in its judicial decisions concerning the right to be forgotten. For example, as indicated in the Court's decision: "*(...) when an internet user entered Mr. Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr. Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.*"[362] The CJEU itself directly

[359]RHÉA, Eddé. Le droit: un outil de régulation du cyberespace? Le cas du droit à l'oubli numérique. *L'Homme & la Société*. 2018, Vol. 1, No. 206, p. 79.
[360] OBERDORFF, Henri. L'espace numérique et la protection de données au regard des droits fondamentaux, Revue du droit public, No. 1, p. 41.
[361] See FABBRINI, Federico, CELESTE, Edoardo. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*. Vol. 21, No. 1, 2020. pp. 55-65.
[362] The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12., para. 14.

indicates the information that the data subject tried to hide from third parties when applying to the Court in order to protect his privacy and reputation.

Thus, Mr. Costeja, who became a "new celebrity" due to the negligent disclosure of the facts by the CJEU, got into an even more difficult situation: now his name is associated with the same information that he tried to hide, no matter how ironic this phenomenon may sound, and gradually more and more this situation aggravates. The problem of Mr. Costeja is that the right to be forgotten is a very controversial tool for the protection of human privacy and reputation, therefore the number of scientific publications dedicated to the topic of the right to be forgotten are growing exponentially. In this context, any researcher who conducts research on the problematic aspects and existing challenges of this right, first of all, studies the story of Mr. Costeja.

At the same time, this phenomena is not new in judicial practice and is known in legal literature as a manifestation of the "Streisand effect", which, in turn, means a paradox when information that is being hidden from third parties attracts even more attention.[363] Various examples can be given to show how the negligence of the Court can lead to the ineffectiveness of the protection of human privacy and reputation in the digital age, and even more – to failure for the plaintiff himself/herself, regardless of the outcome of such a case.[364]

Moreover, the *Google Spain* case clearly illustrates that the "Streisand effect" is able to turn even a little-known person into a real celebrity, regardless of the will of the latter, not to mention the celebrities themselves. Moreover, it is possible that the right to be forgotten can be used as a means of PR, and the "Streisand effect" seems to be the basis for conducting such PR, which makes it possible to attract the attention of third parties to one's personality. For example, one can analyse the same case of *Streisand v. Adelman*[365] from this angle. It is likely that Ms. Streisand filed a lawsuit against the journalist, who photographed her house in Malibu, not because of the desire to remove the photo from the website, but precisely because of the desire to be in the spotlight as a celebrity, regardless of the success of the case itself. If so, then the

---

[363] CARTER, Edward L. The Right To Be Forgotten. Oxford Research Encyclopedia of Communication, Oxford: Oxford University Press, 2016. 3 p.

[364] For example, one of the manifestations of "Streisand effect" is the case of Robert Šlachta. In July 2016, the Czech national court imposed a fine of 8000 CZK on an activist with the pseudonym Tomáš Zelený for insulting the police. He called the former head of the ÚOOZ, Robert Šlachta, an "eared tractor driver" ("*ušatý traktorista*") and mocked the police officers. The event would not have come to wider awareness if it had not been for the fine and the statement of Robert Šlachta, who stated as follows: "Firstly, I never drove a tractor, but a combine harvester, and secondly, the person we investigated spoke this way not only about me, but also about the entire unit". On social networks, jokes and funny collages on the theme of a tractor and a combine harvester immediately began to arise.

[365] Supreme Court of California, *Barbara Streisand Vs. Kenneth Adelman Et. Al.,* Case No. SC077257, County of Los Angeles.

plaintiff's PR was successful: the number of views of the photo of Ms. Streisand's house increased sharply after the American court considered the above case. Of course, this is not a fact, but just an assumption, not devoid of rational explanation.

The example we have given shows that the right to be forgotten may be abused and used not for its purpose by those applicants who are trying to be in the public spotlight. Of course, this should not be allowed, since every human right has its own purpose, and any abuse of human rights should be prohibited. Therefore, the courts, including the CJEU, should be careful in describing the factual circumstances of the case under consideration in order to prevent not only violations of human privacy and reputation, as in the case of *Google Spain* through the "Costeja paradox", but also to prevent the use of the right to be forgotten for the PR purposes.

At the same time, the "Streisand effect", which is associated with the name of Mr. Costeja and, is far from the only case in the judicial practice of the CJEU. For example, the same phenomenon can be seen in the case of *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, where the negligence of not the CJEU itself, but the Advocate General, who did not conceal information of a defamatory nature in his opinion, is already striking: "*On 3 April 2016 a user (...) also published (...) an accompanying disparaging comment about the applicant accusing her of being a 'lousy traitor of the people', a 'corrupt oaf' and a member of a 'fascist party'. (...) namely that the applicant was a 'lousy traitor of the people' and/or a 'corrupt oaf' and/or a member of a 'fascist party'.*[366] As it is possible to notice, Ms. Eva Glawischnig-Piesczek got into the same predicament as Mr. Costeja in the *Google Spain* case.

However, the problem here is even more complex: if I assume that in the case of Mr. Costeja the newspaper of *La Vanguardia* just mentioned an undesirable fact of objective reality for the plaintiff regarding his *"proceedings for the recovery of social security debts"*, then in the case of Ms. Eva Glawischnig-Piesczek, I can see a comment that has no connection with objective reality, but shows only the subjective opinion of the Internet user in a rude and indecent form through such expressions as *"lousy traitor of the people", "corrupt oaf"* and *"a member of a 'fascist party'"*. That is, based on the analysis of the above cases, I can say that the "Streisand effect" is possible not only in the case of truthful but undesirable information, but also in the case of defamatory information, which further aggravates the problem I am considering. Of course, I understand that the personal rights of public figures are being more seriously attacked, and such a person should bear a greater burden and show greater tolerance,

[366] Opinion Of Advocate General Szpunar delivered on 4 June 2019. Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, Recitals 12,14.

as, for example, it was indicated in the case of *Lingens v. Austria*,[367] but nevertheless such public figures are also need to protect their privacy, reputation and dignity, so the greater burden and tolerance does not mean that they do not need to be protected from the "Streisand effect".

It turns out that in the digital world, a person can even be associated with information that is just a product of subjective and/or "groundless" fantasy and/or opinion of any Internet user, regardless of whether the Court considered it as a defamation or not. This shows how far even incorrect information is ready to go in the digital world, and therefore it is necessary to change the approach of formulating factual circumstances both on the part of the CJEU and on the part of other participants in the judicial process (such as, for example, Advocate General) in order to avoid the above cases in the future.

In this regard, the third case, which I will consider below, differs from the previous cases considered. In particular, the Court's judgment in the case of *GC and Others v. CNIL*[368] deserves special attention. In accordance with this case, the Court had to consider the complaint of four applicants (GC, AF, BH and ED), each of whom demanded to remove links in the list of results displayed by the Google search engine in response to a search by their names, leading to web pages published by third parties, which Google, in turn, refused to do. This information can be found in more detail in the paragraphs 25-28 of the case under consideration. So, in accordance with the circumstances of the case "*GC requested the de-referencing of a link leading to a satirical photomontage placed online pseudonymously on 18 February 2011 on YouTube, depicting her alongside the mayor of a municipality whom she served as head of cabinet (...) during the campaign for the cantonal elections in which GC was then a candidate. (...)"*. In his turn, another person *"AF requested de-referencing of links leading to an article in the daily newspaper Libération of 9 September 2008, (...), concerning the suicide of a member of the Church of Scientology in December 2006. AF is mentioned in that article in his capacity as public relations officer of the Church of Scientology (...)"*. As for the third applicant "*BH requested the de-referencing of links leading to articles, mainly in the press, concerning the judicial investigation opened in June 1995 into the funding of the Parti républicain (PR), in which he was questioned with a number of businessmen and political personalities (...)"*. At last, the fourth applicant *"ED requested the de-referencing of links leading to two articles published in Nice Matin and Le Figaro reporting the criminal hearing during which he was*

[367] ECtHR: Judhment of 8 July 1986, *Lingens v. Austria*, App. no. 9815/82.
[368] Court of Justice of the European Union: Judgment of the Court of 24 September 2019. *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*. Case C-136/17.

sentenced to 7 years' imprisonment and an additional penalty of 10 years' social and judicial supervision for sexual assaults on children under the age of 15".[369]

So, it is easy to see that the distinctive feature of the case under consideration is the anonymity of the applicants. Of course, if I compare with the description of the factual circumstances of the previous two cases, then in this case the applicant's confidentiality is protected much more effectively, since it is impossible to find out who exactly the case concerns.

However, there are still circumstances that leave some "clues" for identifying the identity of the applicants themselves and information on the Internet. For example, if I assume that the abbreviated names of applicants are most likely only the first letters of their first and last names and the CJEU does not hide their gender, and the information that applicants would like to delete is in specific links indicating the date of publication of such information (for example, *"on 18 February 2011 on YouTube"* or *"in the daily newspaper Libération of 9 September 2008"*), then the possibility of identifying such persons still remains. That is, the approach of the Court in hiding the applicants' names against the background of the two previous judicial precedents may be considered as commendable, but it still seems to us that there is a room for the Court to refine its practice.

I believe that the most effective way to protect the applicant's privacy would be, firstly, indicating not the first letters of their first and last name, but to use a random letter or a combination of letters, which is typical for the judicial practice of the ECtHR in cases concerning the protection of the privacy and confidentiality of their applicants, such as in the case of *X, Y and Z v. The United Kingdom*[370] or *A and B v. Croatia*[371], or renaming applicant with frequently occurring names, for example, *John and George v. CNIL*, and, secondly, hiding references to publication dates and sources, where the information that is the subject of the case is specified, indicating, for example, not *"in the daily newspaper Libération of 9 September 2008"*, but only *"in the newspaper"* or deliberate distortion of facts that do not affect the merits of the case, or indicating, for example, not "*in the daily newspaper Libération of 9 September 2008*", but "*in the daily newspaper of 11 April 2013*". Of course, this does not mean that the CJEU should hide all the information from the factual circumstances when considering cases of this nature, since in this case it will be impossible to understand on the basis of which facts the Court came to a certain conclusion. It seems to us that the Court should indicate them in such a way that it is impossible to identify the applicant's identity, but without "damaging" the

[369] Ibid, para. 25-28.
[370] ECtHR: Judgment of 22 April 1997, *X, Y and Z v. The United Kingdom*, 75/1995/581/667.
[371] ECtHR: Judgment of 20 June 2019, *A and B v. Croatia,* App. no. 7144/15.

essence of the case at the same time. In other words, the Court should think about the policy of *aurea mediocritas*[372] to ensure an effective *status quo* between the presentation of the facts and the protection of confidentiality of the applicants.

Moreover, the CJEU is the main "creator" of the right to be forgotten the potential to protect human privacy and reputation in the digital world. However, the risk of the "Streisand effect" may negatively affect the judicial practice of the CJEU. As M. Mach correctly notes: "(…) an increase in judgments can be expected over the next few years due to the right having existed for longer and been used more, and parallel with this the Streisand effect could appear in more cases".[373] Consequently, it is important to avoid "Streisand effect" in such new cases, otherwise nobody will apply to the Court for protection of his/her privacy and the right to be forgotten will remain an abstract and vague instrument, without prospects for further development in the dynamic digital world. In this context, as correctly noted by N. Culik and C. Döpke: "In order to prevent negative side effects, like the Streisand effect, requests for deletion must be dealt with confidentially".[374]

A logical question arises: why in the first two analysed cases all information about the applicants is publicly available, but in the last case (i.e. in the case of *GC and others v. CNIL*) some measures are applied to protect the confidentiality of the applicants? The answer to this question will allow us to understand that the "culprits" in violating the confidentiality of the applicants are not only the CJEU or the AG, but also the courts of the EU member States. This is explained by the fact that the basis of the three analysed cases is the request for a preliminary ruling under Article 267 of the TFEU, providing that: *"The Court of Justice of the European Union shall have jurisdiction to give preliminary rulings concerning: (a) the interpretation of the Treaties; (b) the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union; Where such a question is raised before any court or tribunal of a Member State, that court or tribunal may, if it considers that a decision on the question is necessary to enable it to give judgment, request the Court to give a ruling thereon".*[375] This means that the factual circumstances of the case became known to the CJEU from the materials transmitted by the national courts dealing with the aforementioned cases, which in turn did not

---

[372] Aristotle, Nicomachean Ethics II.1

[373] MACH, Martin. Streisand Effect in the Context of the Right to be Forgotten. European Studies – the Review of European law, Economics and Politics. 2022, vol. 9, no. 1, pp. 110–121.

[374] CULIK, Nicolai, DÖPKE, Christian. About Forgetting and Being Forgotten. In HOEREN, Thomas, KOLANY-RAISER, Barbara (eds.) Big Data in Contex. Springer International Publishing, 2018, pp. 21–27.

[375] Consolidated version of the Treaty on the Functioning of the European Union - Part Six: Institutional And Financial Provisions - Title I: Institutional Provisions - Chapter 1: The institutions - Section 5: The Court of Justice of the European Union - Article 267 (ex Article 234 TEC) Official Journal 115 , 09/05/2008 P. 0164 – 0164.

themselves take measures to protect the confidentiality of the applicants before sending their preliminary requests to the Court. Moreover, the national laws of EU Member States provide for mechanisms to protect the confidentiality of their applicants. In particular, article 232 (§3) of the Spanish Organic Law 6/1985 on the Judiciary, which provides that: *«3. Under exceptional circumstances, for motives of public order and the protection of freedoms and rights, Judges and Courts may, via a ruling providing grounds, limit the scope of public access and order all or part of the proceedings to be secret in nature».*[376] In such circumstances, if in the *Google Spain* case the Spanish national court had followed the above provision even before sending the preliminary request to the CJEU, the name of Mr. Costeja Gonzales would not have received such a great resonance.

In this context, the French national court in the case of *GC and others v. CNIL* was even more far-sighted than the national courts of Spain and Austria in the cases of *Google Spain* and *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*. In particular, the French national court clearly understood that when referring a number of questions for a preliminary ruling concerning the right to be forgotten to the CJEU, the protection of the applicants' privacy and reputation is important in order to avoid a new "Costeja paradox" in the future. Before the judicial proceedings, the French Council of State also noted that during the consideration of the case, the names of the applicants will be anonymized *ex officio*, stressing that any party may request anonymization of their data during proceedings in the CJEU.[377] This means that a mere change in the CJEU's case-law is not sufficient to achieve the desired result: a change in the judicial practice of the national courts of the EU Member States themselves is also important and necessary.

6.3.2 What about the ECtHR's judicial approach on the right to be forgotten?

Although I refer to the ECtHR's case law as an example in some places of our research when analysing the CJEU's case law, this does not mean that the above deficiencies do not occur in the ECtHR's judicial practice: it is enough to pay attention, for example, to the

[376] Organic Law 6/1985, On The Judiciary.
[377] REES, Marc. Droit à l'oubli: l'effet Streisand peut être évité dans les décisions de la CJUE. NextBeta [online]. 14th March 2017, [cit. on. 27th December 2023]. Accessible at: <https://www.nextinpact.com/article/25880/103671-droit-a-oubli-effet-streisand-peut-etre-evite-dans-decisions-cjue?fbclid=IwAR3KQQEmXTXq8ifKNeNl8y26xOAta-IfQHUrMkvzYfd5oJPrGD4ncBFzLLg>.

presentation of the factual circumstances in the cases of *Khalili v. Switzerland*[378] and *M.L. and W.W. v. Germany.*[379]

Thus, based on the circumstances of *Khalili v. Switzerland* case, the applicant, Ms. Sabrina Khalili, is a French national, who was born in 1959 and lives in Saint Priest (France). During police check in Geneva in 1993, the police found Ms. Khalili to be carrying calling cards which read: *"Nice, pretty woman, late thirties, would like to meet a man to have a drink together or go out from time to time. Tel. no. (...)"*. In 2001 two criminal complaints of threatening and insulting behaviour were lodged against Ms. Khalili and in 2003 she found out from a letter issued by the Geneva police that the word "prostitute" still figured in the police files, which she demanded to delete from the police records.[380] As one can see, there are a number of similarities in the manner of non-confidential description of factual circumstances between the specified case and, for example, the cases of *Google Spain* or *Eva Glawischnig-Piesczek v Facebook Ireland Limited.*

Another example is the case of *M.L. and W.W. v. Germany*, where the applicants were half-brothers sentenced to life imprisonment by German courts for the murder of a famous German actor. In 2007, they filed a lawsuit against the *Deutschlandradio* radio station, the weekly magazine *Der Spiegel* and the daily newspaper *Mannheimer Morgen*, demanding the removal of their personal data on the respective Internet websites where information about the applicants' crime had been posted, which was later rejected by the German Federal Court. The German court justified its judgment by the fact that one of the aims of the mass media is to participate in the formation of democratic opinion by making available to the public old news that has been preserved in their archives, so the applicants appealed to the ECtHR on the basis of Article 8 of the European Convention on Human Rights (the right to respect for private life).

However, when considering the case, the ECtHR makes the same mistake as the CJEU did in *GC and Others v. CNIL*. In particular, if one pay attention to the paragraph 7 of the Court's judgment, it is possible to notice, how this judicial decision, though hiding the names of the applicants, but at the same time contains the facts, allowing to easily identify the applicants. In particular, the Court specifies the following: "*The applicants are half-brothers. On 21 May 1993, following a criminal trial based on circumstantial evidence, they were sentenced to life imprisonment for the 1991 murder of W.S, a very popular actor. They lodged an appeal on points of law which was dismissed in 1994. On 1 March 2000 the Federal*

[378] ECtHR: Judgment of 18 October 2011, *Khelili v. Switzerland,* App. no. 16188/07).
[379] ECtHR: Judgment of the Court of 28th June 2018, Case of *M.L. and W.W. v. Germany* (Applications nos. 60798/10 and 65599/10).
[380] *See* Press release issued by the Registrar of the Court ECHR 195 (2011), 18.10.2011

Constitutional Court decided not to entertain their constitutional appeals (nos. 2 BvR 2017/94 and 2039/94) against the decisions of the criminal courts. An application to the Court lodged by the applicants concerning those proceedings (no. 61180/00) was rejected on 7 November 2000 by a three-judge committee on the grounds that the applicants had not lodged their constitutional appeals in accordance with the procedural rules laid down by the Federal Constitutional Court Act (unpublished decision)".[381] Of course, based on the facts of the case, in particular the abbreviation "*W.S.*" and the case numbers in the German courts' judgments, I can easily determine that the case is related to information about the murder of the famous German actor *Walter Sedlmayr*. Since I was able to find information about the victim of the crime, it is also easy to determine who the applicants of the case are: just the simple search for "*Walter Sedlmayr's murder*" in the Google search engine allows to identify the applicants. So, the search shows the following information, which can be found on the English version of Wikipedia: "On 21 May 1993, two half-brothers, *Wolfgang Werlé* and *Manfred Lauber*, former business associates of Sedlmayr, were found guilty of his murder and sentenced to life in prison. The killers were released from prison in 2007 and 2008".[382] Thus, as a result of a careless approach in describing the factual circumstances on the part of the ECHR, it became possible to easily identify the identity of the applicants in the specified case: if "*M.L.*" is *Manfred Lauber*, then "*W.W.*" is *Wolfgang Werlé*. As one can see, hiding the names of the applicants does not guarantee that they cannot be identified, so both the CJEU and the ECtHR should be very careful in presenting the facts of the cases in the future.

There are other cases in the case law of the ECtHR when the Court does not protect the applicants' data and thereby puts them at risk of a new "Streisand effect". In particular, such court cases include the cases of *Fuchsman v. Germany* and *Węgrzynowski and Smolczewski v. Poland*, to which M. Mach also drew attention in his scientific publication.[383] Indeed, when studying these cases, I receive too much information about the applicants, while they applied to the Court in order to protect their privacy and reputation. So, when analysing the case of *Fuchsmann v. Germany*, one can see that: "*The applicant, Boris Fuchsmann, is a German national who was born in 1947 and lives in Düsseldorf (Germany). He is an internationally active entrepreneur in the media sector and runs the company Innova*

---

[381] ECtHR: Judgment of the Court of 28th June 2018, Case of *M.L. and W.W. v. Germany* (Applications nos. 60798/10 and 65599/10), para. 7.

[382] Walter Sedlmayr. Wikipedia [online]. [cit. on 28th December 2023] Accessible at: <https://en.wikipedia.org/wiki/Walter_Sedlmayr>.

[383] MACH, Martin. Streisand Effect in the Context of the Right to be Forgotten. *European Studies – the Review of European law, Economics and Politics.* 2022, Vol. 9, No. 1, pp. 110–121.

Film".[384] As one can see, it is already clear who the applicant is in this case. Further, the Court describes the factual situations of the case as follows: "*Mr Fuchsmann, who was one of the owners of a broadcasting company in Kiev, had ties to Russian organised crime, according to the FBI and European law enforcement agencies. The article further reported: that a FBI report had described Mr Fuchsmann as an embezzler, whose company in Germany was part of an international organised crime network; that he was barred from entering the United States; and that his company Innova was part of a Russian organised crime network, according to U.S. and German law enforcement agencies*".[385] In this case, the Court did not find a violation of Article 8 of the ECHR (i.e. the right to private life), but I affirm that regardless of whether the Court found a violation or not, in cases concerning the right to private life there is a serious problem of protecting the applicant's confidentiality. By ensuring the applicant's confidentiality when considering such cases, the Court, as a guarantor of human rights, will itself show its respect for the human rights that it protects. I believe that such a practice will in no way upset the balance between freedom of expression and information and the right to private life in favour of the right to private life. At the same time, it is possible to simultaneously protect the confidentiality of the applicant and describe the factual circumstances in such a way that anyone who wants to read the judicial decision can get acquainted with the circumstances of the case and understand the legal reasoning of the Court. This is the way the ECtHR should move when describing the factual circumstances of the case in its judicial decision.

In another similar case, in the case of *Węgrzynowski and Smolczewski v. Poland,*[386] the applicants' confidentiality is also not protected. We will find out their names, place of residence as well as the name of the newspaper where the article was published. At the same time, the Court hides the data of journalists in its judicial decision. And here the question arises: why does the Court hide the data of journalists, realizing the importance of ensuring their confidentiality, but does not hide other important data, for example, the names of the applicants or information on the newspaper, etc.? In this context, the logic of the Court is not entirely clear on the description of the factual circumstances of this case. I believe that the Court most likely does not have a uniform policy on how to effectively ensure the applicants' confidentiality, and

---

[384] *See:* Case of *Fuchsmann v. Germany* (Application no. 71233/13). Judgment Strasbourg, 19 October 2017. Final 19/01/2018, Recital 7 // Available at: https://hudoc.echr.coe.int/eng#{"itemid":["001-177697"]}. *See also:* Press Release issued by the Registrar of the Court, ECHR 313 (2017) 19.10.2017.

[385] *Ibid.*

[386] Case of *Węgrzynowski and Smolczewski v. Poland* (Application No. 33846/07) Judgment Strasbourg 16 July 2013 Final 16/10/2013 // Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-122365%22]}

therefore, in various cases, the Court takes different approaches to describing the factual circumstances. Such a difference can be noticed when studying the cases, I have indicated in this research.

The above cases are capable of weakening the principle emerging from the observations of ECtHR that the right of privacy (Article 8 of the ECHR) and right for freedom of expression (Article 10 of the ECHR) should be treated equally and the legal solutions should balance the rights, which, in turn, was emphasized by the Court in such cases as, for example, *Axel Springer AG vs. Germany*, *Von Hannover vs. Germany (nr 2)*, *Delfi AS vs. Estonia* and *Pauliukienė and Pauliukas vs. Lithuania*.[387] This practice is the natural consequence of the fact that from the very beginning the Court did not properly take care of protecting the applicant's privacy and hiding information that was the subject of the dispute in the case under consideration. The problem is that a lot of unnecessary information is disclosed in court cases, which makes it easy to identify both the applicants and the information they wanted to hide. That is, in this case, freedom of information prevails over the protection of the applicant's privacy and reputation, while the Court must ensure their effective coexistence.

6.4 The global reach of the right to be forgotten through the lenses of the CJEU

One of the most controversial issues of regulating the right to be forgotten is its scope of territorial application. Another issue as Advocate General *Szpunar* stated in his Opinion on the case of *Google v. CNIL* is the territoriality principle,[388] which is highly debatable. In turn, M. Taylor even considers the global removal of information as an illustration of ineffective jurisdictional excess.[389] Therefore, it is not surprising that the national DPAs and the courts have encountered with serious difficulties in interpreting and applying of the right to be forgotten, which was the reason for a large number of preliminary requests sent to the CJEU. Thus, in September 2019 the CJEU accepted the case of *Google v. CNIL*[390], the request for a

[387] *See:* Axel Springer AG vs. Germany, p 87; Von Hannover vs. Germany (nr 2), p 106; Delfi AS vs. Estonia p 82; Pauliukienė and Pauliukas vs. Lithuania, EIKo 5.11.2013, nr 18310/06, p 51

[388] Opinion Of Advocate General Szpunar delivered on 10 January 2019, para. 45.

[389] TAYLOR, Mistale. Google Spain Revisited: The Misunderstood Implementation of a Landmark Decision and How Public International Law Could Offer Guidance. *European Data Protection Law Review*. 2017, Vol. 3, No. 2, pp.195-208.

[390] Court of Justice of the European Union: Case C-507/17 *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL),* ECLI:EU:C:2019:772 (hereinafter – *"Google LLC v CNIL"*).

preliminary ruling on which the above case is based was specifically concerned with the geographical scope of the right to be forgotten. Many scholars interpreted the judgment of the *CNIL* case as a territorial restriction on the right to be forgotten. In particular, as M. Samonte believes: "By explicitly limiting the territorial scope of the right to be forgotten, the Court may seem to have inadvertently limited the impact and protective effect of this right."[391]

However, is it possible to consider such an interpretation as unambiguous? I believe that it is not, taking into account the open possibility of interpreting the *CNIL* case in a different way - as creating conditions for a global right to be forgotten, i.e. as "a floor, not a ceiling".[392] This trend has become even more clearly visible in the case of "*Piesczek v. Facebook*", where the Court ruled that: "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from: (...) – ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law" .[393]

6.4.1 The pre-*CNIL* situation and the main problems

Despite the apparent progressiveness of the *Google Spain* judgment in the field of the EU human rights protection, it nevertheless gave rise to many problems that need to be solved and thus determined the trend of further development of the case law of CJEU in the field of digital rights. In this context R. Weber rightly notes that: "a clearer picture of the actual objective of a new fundamental right is necessary. The proclamation of a right to be forgotten as such does not suffice. It recalls the myth of Pandora's box: Impelled by her natural curiosity, Pandora opened the box and all the evils contained in it escaped".[394] In this context naturally arises the question about what are the main issues that flow out of the *Google Spain* judgment?

---

[391] SAMONTE, Mary. Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law. EuropeanLawBlog [online]. 29th October 2019. [cit. on. 25th December 2023]. Accessible at: <https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/>.

[392] Ibid.

[393] Court of Justice of the European Union: Judgment of 3th October 2019. *Eva Glawischnig-Piesczek v Facebook Ireland Limited.* Case C-18/18, para. 55.

[394] WEBER, Rolf. The Right to Be Forgotten: More Than a Pandora's Box? *JIPITEC*, 2011, Vol. 120, pp.120-130.

This question is correctly answered by O. Gstrein, who notes that there are three questions one of which the territorial scope of the application.[395]

The issue of territorial scope of GDPR itself was also left open by the CJEU. For example, it is unclear whether the "right to be forgotten" applies only within the EU? Whether it applies to search engines running on the .com domain or other domains outside the EU as well?

By introducing new standards for the protection of personal data, the CJEU forces any Internet company to follow the rules set out in this judgment, even if such a company *de facto* operates outside the EU. Obviously, the Court's judgment should raise questions about the extraterritorial nature of both the right to be forgotten and the GDPR in general. The questions of the interpretation of the DPD raised in preliminary ruling were assessed in the light of the GDPR "in order to ensure that its answers will in any event be of use to the referring court".[396] So, the Court dispelled doubts about the possibility of transferring the conclusions of this case to the new legal regime, but it did not resolve the issue of the territorial application of this legal instrument.

Thus, the CJEU, having made a judgment that does not have any evaluation criteria or guidelines for national courts on how to implement it, has opened a way for endless judicial debate. Problems related to the implementation of this judgment of the CJEU by the national courts of the EU member States have caused the Court to start receiving preliminary requests. As Y. Padova states: "The 'right to be forgotten' (…) continues its judicial saga as it is being examined by the very same Court that created it, following the submission of 11 preliminary questions by the French Council of State before the Court of Justice of the European Union (CJEU)".[397]

6.4.2 The *Google v. CNIL* case

In 2015 CNIL notified Google of its obligation to remove links from all versions of its search engine worldwide. The CNIL held the position that removing links about an individual on the French version of Google is not enough to protect human rights. To do this, the Google

[395] GSTREIN, Oskar J. The Judgment That Will Be Forgotten'. Verfassungsblog: On Matters Constitutional [online]. 25th September 2019. [cit. on. 25th December 2023]. Accessible at: <https://verfassungsblog.de/the-judgment-that-will-be-forgotten/>.
[396] Case C-507/17 *Google LLC v CNIL*, para. 41.
[397] PADOVA, Yann. Is the right to be forgotten a universal, regional, or 'glocal' right? *International Data Privacy Law*. 2019. Vol. 9, No. 1, p. 15.

should exclude links from the list everywhere. The CNIL considered it insufficient to exclude links from all extensions operating in the EU, as well as from all search queries conducted in France, since Internet users located in France can still access other versions outside the EU. Although the Google refused to remove face data from all versions of its search engine and continued to restrict link redirects only in versions of its search engines with domain extensions within the EU. In March 2016, Google tried to compromise with CNIL and somehow to change the situation. It proposed the implementation of geo-blocking meaning that "internet users would be prevented from accessing the results at issue from an IP (Internet Protocol) address deemed to be located in the State of residence of a data subject (…), no matter which version of the search engine they used".[398] As K. Walker points out: "That means that if we detect you're in France, and you search for someone who had a link delisted under the right to be forgotten, you won't see that link anywhere on Google Search—regardless of which domain you use. Anyone outside the EU will continue to see the link appear on non-European domains in response to the same search query".[399] The CNIL found suggested measure to be insufficient for the solution of the situation. The Commission's order rejected Google's compromise position and mentioned that "only delisting on all of the search engine's extensions, regardless of the extension used or the geographic origin of the person performing the search, can effectively uphold this right. The solution that consists in varying the respect for human rights on the basis of the geographic origin of those viewing the search results does not give people effective, full protection of their right to be delisted."[400] The Google turned to French Council of State[401] for the fine, which was imposed by CNIL.[402] The latter observed that a user located in a Member State is able to use the international version of the search engine instead of the one tailored for its specific country, that common databases and a common indexing process connects the international version with all the nation-specific versions of the search engine, and that cookies created by a user while visiting a specific version of the search engine would be automatically shared with all other versions of the search engine.[403] The French Council of State (hereinafter – the "FCoS") stated that all processing of personal data done by the Google should be seen as a single combined process and that therefore no distinction should apply between the

[398] Ibid, p. 32.
[399] WALKER, Kent. A Principle That Should Not Be Forgotten. Google Blog. [online]. 19th May 2016. [cit. on. 25th December 2023]. Accessible at: <https://blog.google/around-the-globe/google-europe/a-principle-that-should-not-be-forgotten/>.
[400] Commission nationale de l'informatique et des libertés [CNIL] Google, Inc., No. 2016-054, Mar. 10, 2016, 3 (Fr.): 53.
[401] Hereinafter - FCoS.
[402] Case C-507/17 *Google LLC v CNIL*. para. 32-34.
[403] Ibid, para. 36-38.

nation-specific versions of the search engine and the international one, for the matter of enforcing data protection rights.[404] The Google argued that the Court in the *Google Spain* case did not define the territorial scope of the right to be forgotten.[405] The FCoS referred questions to the CJEU for a preliminary ruling on the scope of articles 12 (b) and 14 (a) of the DPD and asked the CJEU for guidance on the territorial scope of de-referencing. Three options were identified: 1) de-referencing on all language versions of the search engine; 2) EU-wide de-referencing; and 3) de-referencing of links only in such a member State and from such a language version of the search engine for which the removal request was submitted, which is mainly due to the geo-blocking of search results in other language versions of the search engine.

6.4.3 Tackling the "regional" option of the right to be forgotten

In *CNIL* case the CJEU has been faced with the dilemma of choosing between recognizing the global application of the right to be forgotten, which would ensure full protection of this right, and between recognizing the non-universal application of the right to be forgotten, thereby reducing the level of protection of this right, but taking into account the "digital sovereignty" of states. At first glance, the Court chooses the latter. The Court pointed out that many third States either do not acknowledge the right to be delisted or "have a different approach" to it,[406] meaning that they might decide to settle the dispute with the right to freedom of information in favour of the latter.[407] But that it is by no means obvious from the wording of the Directive and the GDPR that the EU legislature has decided to grant a scope for the right in question that extends beyond the territory of the member States.[408]

Next, the Court highlighted the difficulties of global redirection, noting that the public interest in access to information varies significantly depending on third States, so the balance of fundamental rights will also differ. Article 17 (3) of the GDPR gives the power to the EU and to authorities of Member States to balance between the mentioned conflicting interests, but not for situations where an extra-territorial application is deemed as more desirable and effective,[409] nor are national supervisory authorities within the EU equipped with proper codes of conduct and mechanisms for the balance of conflicting interests in an extra-territorial

[404] Ibid, para. 37.
[405] Ibid, para. 38.
[406] Ibid, para. 59.
[407] Ibid, para. 60.
[408] Ibid, para. 62.
[409] Ibid, para. 61-62.

situation.[410] So the GDPR does not offer an obligation for a search engine to apply the right to de-referencing on a global scale.[411] In accordance with its approach in the Google Spain case, the CJEU concluded that under EU law there is no obligation to cancel the reference for all language versions of the search engine.[412] The Court preferred a review of the law on an EU scale.[413]

Besides, the Court essentially expresses respect for the right of other states to strike a different balance between the right to data protection and freedom of information. The Court tried to provide the highest possible level of protection of the right to data protection, while respecting the international comity[414] and legal diversity. Although even the best intentions of the Court in the matter of international cooperation reduce to nothing when one evaluates such a position from the point of view of the effectiveness of the protection of the right itself. The fact is that it is not possible to fully and effectively enforce this right at the local level because it would give Internet users who search information outside the EU an opportunity to still have access to links that do not apply in the EU. The CJEU is also aware of this fact. It points out that the purpose of the EU data protection law is to guarantee a high level of protection throughout the EU.[415] This means that the assertion of the legality of only non-universal application of the right to be forgotten could interfere with the EU's goal of ensuring a high level of personal data protection. In its turn, the WP29 stated that "in order to give full effect to the data subject's rights as defined in the Court's ruling, delisting decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting delisting to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects

---

[410] Ibid, para. 63.
[411] Ibid, para. 64-65.
[412] Ibid, para. 64.
[413] Ibid, para. 66.
[414] A clear example of application of the international comity principle in the field of personal data protection may serve *the Brief of the European Commission on behalf of the European Union as Amicus Curiae in support of Neither Party* in the case of *United States of America v. Microsoft Corporation*, where the European Commission in its, stated that: "Any domestic law that creates cross-border obligations—whether enacted by the United States, the European Union, or another state—should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union's foundational treaties and case law enshrine the principles of "mutual regard to the spheres of jurisdiction" of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law" (*See*: p. 7). Accessible at. [online]: <https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf>.
[415] Recitals 10, 11 and 13 of the GDPR.

according to the ruling".[416] The WP29 added, that "in practice, this means that, in any case, de-listing should also be effective on all relevant domains, including .com".[417]

The approach of the CJEU on the admissibility of the local application of the right to be forgotten was recognized by some researchers as a victory for Google for global freedom of expression.[418] Although the Court's judgment itself, at first glance, considers the local application of this right in conjunction with geo-blocking measures to be an acceptable solution in this situation, it should be noted that this is a direct path to the fragmentation of the Internet. The risk of such fragmentation highlights J. Daskal, who argues that: "(…) countries with less liberal views about freedom of speech and expression can effectively create a fenced version of the internet based on arbitrary parameters (...)".[419] In addition, the commitment to the "local" application of the right to be forgotten in the position of the CJEU is not so clearly expressed. The existence of such an unambiguous position that would exclude the global application of this right would mean the weakening of the protection of the right under consideration by the Court itself. It seems to us that the CJEU does not consolidate such an unambiguous position today and is unlikely to adopt such a consolidation in favor of the "local" application of the right to oblivion in the near future.

6.4.4 "Universal" application of the right to be forgotten?

It is noteworthy that a categorical prohibition of the possibility of global application of the right to be forgotten in the judgments is unlikely to be found. On the contrary, in detailed analysis of the Court's considerations in the *Google v. CNIL* case one can see indirect recognition of the possibility of global application of the law in question. As one can see the Court made clear that while the EU law does not currently require worldwide de-referencing, "it also does not prohibit such a practice"[420]. The CJEU stated that while nothing in EU law can be interpreted as imposing a global enforcement of the right to de-referencing, national

[416] WP29 Guidelines on the Implementation of the CJEU Judgment on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez' C-131/12, adopted on 26 November 2014, p.3.
[417] Ibid.
[418] COWBURN, Pam. Google win in right to be forgotten case is victory for global freedom of expression. Article 19 [online]. 24th September 2019. [cit. on 25th December 2023]. Accessible at: <https://www.article19.org/resources/google-win-in-right-to-be-forgotten-case-is-victory-for-global-freedom-of-expression/>.
[419] DASKAL, Jennifer. SPEECH ACROSS BORDERS. Virginia Law Review, 2019, Vol. 105, No. 8, pp. 1605–1666.
[420] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 September 2019. *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL),* Case C-507/17, para. 72.

authorities are not prevented from demanding such an extensive implementation on a case-by-case basis, should this not be seen as clearly threatening for the right to freedom of information of the global population.[421] It is not known whether unintentionally, through the vague wording of the provision or completely intentionally, the CJEU thereby provides an opportunity for global protection (...) of the right to information of the global population. This in itself shows that the Court is not at all categorical about the possibility of protecting individual rights on a global scale. As M. Zalnieriute points out: "By leaving the door to extraterritorial de-referencing wide open, the CJEU continues to pursue its post-Snowden hard-line stance on data privacy in a manner that is likely to transform the data privacy landscape".[422]

Even a careful analysis of the GDPR shows that the legal act does not contain a provision that would directly limit its scope. Moreover, Article 3(2)(b) of the GDPR states that the GDPR applies to monitoring user behaviour occurring in the EU, even if the controller is not registered in the EU. Considering the territorial applicability of the GDPR, the CJEU in the CNIL case does not change the broad interpretation of article 3(1) of the GDPR, given in *Google Spain*, where it was extended to the processing of personal data of data subjects located in the EU by a controller not registered in the EU, if the processing actions were related to the offer of goods or services. Therefore, the position of the CJEU that the EU legislature does not grant the rights enshrined in the GDPR outside the territory of EU member States is questionable.[423]

The Court first noted that in a globalised world, even access to information specified in search results by an Internet user located outside the EU can have immediate and significant consequences for the victim in the EU.[424] The CJEU stressed that the FCoS considers Google as a single entity when it comes to the processing of data connected to natural persons such as French/EU citizens.[425] It also acknowledged the validity of the argument that a global application of the right to be delisted would certainly meet the declared aim of the GDPR - "to guarantee a high level of protection of personal data" within a global online environment that facilitates the flow of information across national boundaries to a degree never witnessed before".[426] In this way, the Court gives legitimacy to global de-referencing. As P. Dixit states: "The judgment in favour of Google, allowing dereferencing only around the EU and not

---

[421] Ibid.
[422] ZALNIERIUTE, Monika. Google LLC v. Commission nationale de l'informatique et des libertés (CNIL). *American Journal of International Law*, 2020, Vol. 114., No. 2. pp. 261 – 267.
[423] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 September 2019. *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL),* Case C-507/17, para. 62.
[424] Ibid, para. 57.
[425] Ibid, para. 52.
[426] Ibid, para. 54-58.

globally stands criticized, however the judgement when read intrinsically allows the Member States to weigh between the right to be forgotten and the right to freedom of information and if in the interest of the national public good, there be a reason to demand for dereferencing globally, such an order can be made. This proves that there is no complete bar and limitation to the right to be forgotten in the EU".[427]

Besides, the Court subordinates the processing of data by Google on all its domains to the GDPR jurisdiction, ruling that Google should be considered as performing a single act of processing personal data.[428] Despite the Court's considerations that EU law does not provide for an obligation to implement the revocation of reference on a global scale, the Court nevertheless points out that the EU legislature has the competence to establish an obligation if it chooses to do so.[429] Such a view is probably based on the possibility of extending EU law outside the EU when extraterritorial application of the EU law may be warranted by the necessity of properly defending the Union's values. [430]

The Court also noted that while EU law does not require the abolition of reference on a global scale, it also does not prohibit such practices. Therefore the CJEU itself in its subsequent case law gave a positive answer to the question whether an order to a host provider to delete unlawful content pursuant to article 15(1) of the Directive 2000/31/EC [431] may have a worldwide effect.[432] In the *Google v. CNIL* case, the Court is of the opinion that a national supervisory or judicial authority may, after balancing the rights and interests of the subjects involved in the light of national standards for the protection of fundamental rights, order the search engine operator to remove the link to all versions of the search engine.[433] The CNIL, in a press release issued after the Court's judgment in the case under consideration, highlighted this competence, but recognized that it was only competent to order worldwide renaming "in some cases".[434]

---

[427] DIXIT, Priyanshi. Will The Internet Remember You Forever? Right To Be Forgotten And Its Territorial Limits [online]. IIPRD, 23th November, 2019 [cit. on. 25th December 2023]. Accessible at: <https://www.iiprd.com/will-the-internet-remember-you-forever-right-to-be-forgotten-and-its-territorial-limits/>

[428] Ibid.

[429] Ibid.

[430] Art. 2 and 3(1) of the Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01.

[431] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) OJ L 178, 17.7.2000, p. 1–16.

[432] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 September 2019. *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL),* Case C-507/17, para. 49-53.

[433] Ibid., para. 72.

[434] CNIL, '"Right to be forgotten": the CJEU ruled on the issue' (Commission Nationale de l'Informatique et des Libertés, 24 September 2019)

The Court leaves space for the possibility of a global application of the right to be forgotten, as defined by national DPA or national courts of the EU member states. In doing so, it provided national DPA and national courts with some space for manoeuvre so that they could respond to the circumstances of a particular case. However, deviation from the EU-wide dereferencing standard is only possible in exceptional cases. But the most visible drawback of the judgment is that the Court does not give any indication in which exceptional cases a deviation from the local application of the right to be forgotten is possible. Nor does it provide the criteria by which national DPA or national courts should be guided in determining or evaluating these cases or their circumstances. The Court's above-mentioned assertions point to its continued efforts to preserve the possibility for Member States to apply the right to be forgotten globally by allowing the adoption of national laws that provide the basis for effective regulation of privacy and data protection.

It should be noted that the issue of universal application of EU data protection legislation was also considered in the case *Piesczek v Facebook*. The cases of *Piesczek v. Facebook* and *Google v. CNIL* considered various EU legislative acts, but both concerned precisely the territorial scope of injunctions against internet intermediates.[435] In *Piesczek v. Facebook*, the CJEU made some changes in its approach compared to *Google v. CNIL*. In accordance with the circumstances of the *Piesczek v. Facebook* case, a Facebook user published an article about the social security of refugees and included several slanderous comments to Eva Glawischnig-Piesczek, a member of the Austrian Green Party. According to the judgment of the Austrian courts, Facebook has disabled access to content in Austria. The Austrian Supreme Court asked the CJEU to consider whether Article 15 of the E-Commerce Directive allowed the injunction to be extended globally as well as to other identical statements and those with an equivalent meaning.

The AG recommended the CJEU to adhere to the position that the court injunction should apply worldwide however even if such injunction should cover identical statements by any Internet user, that it should only apply to equivalent statements by the user who is the author of the unique illegal content.[436] As in the case of *Google v. CNIL*, the importance of a balance between fundamental rights was again emphasized, for which the AG proposed criteria for

[435] MAZÚR, Ján, PATKYOVÁ, Mária T. Regulatory Approaches to Facebook and Other Social Media Platforms: Towards Platforms Design Accountability. *Masaryk University Journal of Law and Technology*, 2019, Vol. 13, No. 2, pp. 219-241.
[436] Opinion of Advocate General Szpunar delivered on 4 June 2019. Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, para.109.

monitoring of 'equivalent' information: it should be "clear, precise and foreseeable"[437]. The recommended criteria were not reflected in the CJEU judgment itself. The CJEU allows monitoring for both identical and equivalent information across *all users* of an online platform, but it does not point out any qualification for equivalent information. The CJEU's judgment does not mention, that the right to personal data protection should be balanced with other fundamental rights. In the judgment of *Piesczek v Facebook* the CJEU only indicated that the monitoring of such information shall be restricted to "information conveying a message the content of which remains essentially unchanged compared with [unlawful content]".[438] But this wording added ambiguity to the question and raised the question on what information should be subject to monitoring, since it is impossible to clearly specify what "essentially unchanged" means.

As opposed to *Google v. CNIL* concerning the territorial scope of injunctions the CJEU held that Member States could issue them against intermediaries with worldwide effect *"*within the confines of public international law".[439] To substantiate its conclusions regarding the admissibility of global injunctions in the *Piesczek v. Facebook* case, the CJEU relied primarily on article 18(1) and recital 52 of the ECD. According to the recital 52 of the ECD, Member States must ensure that *"*appropriate court actions*"* are available to guarantee victims effective access to damage which may arise in connection with "information society services", which *"*is characterised both by its rapidity and its geographical extent*"*.[440] Article 18(1) of the ECD provides for the availability of court actions under national law against information society services, allowing for *"*the rapid adoption of measures…designed to terminate any alleged infringement and prevent any further impairment of the interests involved*"*. The CJEU noted that in implementing article 18(1) of the ECD, Member States have a *"*particularly broad discretion in relation to the actions and procedures*"* for such measures.[441] Further, the CJEU held that given that the means and measures provided for in article 18(1) of the ECD were directly oriented to cease *any* alleged violation and to prevent *any* future deterioration of the conditions of the interested parties involved, no restrictions should be allowed on the scope of application of such means and measures. The CJEU also found that because the ECD did not limit the scope, territorial or otherwise, of the measures which a Member State could adopt

[437] Ibid, para. 71.
[438] Ibid.
[439] Ibid, para. 53.
[440] Ibid, para. 52
[441] Court of Justice of the European Union: Judgment of 3th October 2019. *Eva Glawischnig-Piesczek v Facebook Ireland Limited.* Case C-18/18, para. 28-29.

under Article 18(1) or otherwise, the ECD does not prevent Member States from issuing injunctions with worldwide effect. [442]

In the *Google v. CNIL* case the CJEU noted that neither the provisions of the DPD nor the provisions of the GDPR imply that in order to ensure a high level of data protection throughout the EU, these provisions must apply outside the EU. Although in the *Piesczek v. Facebook* case the CJEU found that a Member State court could issue orders that not only extend across the EU but also globally. As one can see the CJEU (almost simultaneously) demonstrated different approaches to the two EU tools, which are similar in that both require intermediaries to block or filter content available to end users. However there is no obvious discrepancy between the approaches reflected in the cases of *Google v. CNIL* and *Piesczek v. Facebook:* the CJEU in *Google v CNIL* did not rule out a global de-referencing order and accepted that it would be possible.[443] The CJEU analysed the issue of establishing "any limitation, including a territorial limitation, on the scope of the measures which Member States are entitled to adopt" in relation to information society services.[444] The Court stated that EU law does not exclude that these measures will lead to global.[445] The CJEU point out that "in view of the global dimension of electronic commerce, the EU legislature considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at international level".[446] The Court also mentioned that "it is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules."[447] So CJEU gives an opportunity to national courts to establish obligations to remove information covered by the injunction or to block access to that information worldwide.[448] And this is a continuation of the trend laid down in the *Google v. CNIL* case, rather than shift in the Court's approach regarding the territorial scope of the right to be forgotten. In this framework the right to be forgotten, which develops almost exclusively as a result of the law-making of the CJEU in conditions when "digital imperialism" becomes the goal of many developed countries, becomes a kind of tool for asserting its digital power for the EU far beyond its borders. Of course, one can considers it as an advantage, but I tend to believe that this is disadvantage if

---

[442] Ibid., para. 49-50.
[443] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 September 2019. *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL),* Case C-507/17, para.72.
[444] Court of Justice of the European Union: Judgment of 3th October 2019. *Eva Glawischnig-Piesczek v Facebook Ireland Limited.* Case C-18/18, para.49.
[445] Ibid., para. 50.
[446] Ibid., para. 51.
[447] Ibid., para. 52.
[448] Ibid., para. 53.

taking into account that the CJEU's judgment, which are "aimed" at extending their rules to the global digital order, nevertheless do not have "coercive force". This means that making judgments that are not destined to become a reality can significantly reduce the credibility of the CJEU itself.

6.4.5 Finding a balance between global and local approaches to the right to be forgotten

Life in today's global digital society does not recognize national borders, primarily because of the "extra-territorial" nature of information and the Internet itself. And the legal regulation of this sphere willy-nilly must take this fact into account. Otherwise, the application of this right exclusively on the territory of the EU will not make any sense. In paragraph 72 of the judgment of *Google v. CNIL* case, the CJEU itself acknowledged that the Union-wide exclusion of search results may not be sufficient to protect privacy rights in some cases. And this consideration implies the need to extend the EU right to data protection beyond the EU as well. This could be an ideal opportunity for the EU to justify extending its law outside the EU.

As pointed out by Ch. Kuner: "the globalised environment of the internet, shaped by a combination of hard law from multiple jurisdictions and private soft law, is the ideal benchmark for the ambitions of EU law".[449] But the CJEU, while supporting the possibility of a global application of the right to be forgotten, does not offer anything new. Even before the ruling on the *Google Spain* case some jurisdictions, for example such as Russia, Mexico, Brazil and so on, have started granting the application of the similar right. Therefore, this can be considered quite an expected approach; I can say support for the global trend. If only the local application of the right to be forgotten is recognized by the CJEU it means the ignoring of this fact.

Nevertheless, the extraterritorial application of the EU Data Protection law poses a number of problems. The adoption of national data protection standards outside the boundaries of EU jurisdiction may conflict with the obligations of international comity and the need to respect the diversity of existed legal systems. In fact, the balance between the right to be forgotten, freedom of information, and freedom of speech is established differently in jurisdictions, even if States recognize faith in democracy, the rule of law, and human rights. Moreover, the application of data protection standards outside the borders of the EU jurisdiction may eventually be negated by the opposite requirements that are established in other

[449] KUNER, Christopher. The Internet and the Global Reach of EU Law. In CREMONA, Marise, SCOTT, Joanne (eds.). EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law. Oxford: Oxford University Press, 2019, pp. 112–145.

jurisdictions.[450] That is why some scholars recommend the EU lawmakers do not extend the scope of right to be forgotten beyond the EU.[451]

Another constraint on the global application of the right to be forgotten in particular and the EU data protection law as a whole may be the principle of international comity, which is understood as a mutual recognition of the validity of foreign law out of good will. According to this principle EU courts should not generally impose European legal norms on jurisdictions outside the EU.[452] In the *Glawischnig-Piesczek* case the Court stressed the importance of consistency between EU law and international rules, without naming the principle of international comity.[453] The CJEU made possible for Austrian courts to imposing obligations to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.[454] However, Advocate General Szpunar in the *Google v. CNIL* case pointed specifically to the principle of international comity as incompatible with the global application of the right to be forgotten.[455] And ensuring global compliance with Article 17 GDPR must take this principle of international comity into account. Of course, this is somewhat difficult, given that the "imposition" of their own standards for the protection of digital rights is inherent not only in the EU, but also in other states that are trying to extend the rules of their jurisdiction to information and data.

I believe that the CJEU is not faced with the dilemma of choosing between local and global application of the right to be forgotten, but rather with the question of developing criteria that can pragmatically solve the problems of modulating the impact of the EU data protection law outside the EU borders. However, the choice (or rather the need) for the global application of this right will undoubtedly be constantly "hanging" over the CJEU: criticism of the "imposition" of its data protection standards on other States that have their own claims to control data, contrary to the obligations of international comity and the need to respect the diversity of legal systems. And this is one of the many challenges of the global application of data protection standards. And it is possible (and in fact it is already clear) that, in view of the increasing tension between these opposite trends, the efforts of the CJEU will not be aimed at choosing one of the

---

[450] FABBRINI, Federico, CELESTE, Edoardo. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*. Vol. 21, No. 1, 2020. pp. 55-65.
[451] PIRKOVA, Eliška, MASSÉ Estelle. EU Court decides on two major "right to be forgotten" cases: there are no winners here. AccessNow [online]. 23th October 2019. [cit. on. 23th December 2023]. Accessible at: <https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/>.
[452] MCCARTHY, Hugh, COX, Arthur. Expanding the GDPR's journalism exemption - is all the world a stage? *Privacy and Data Protection*. 2019. Vol. 14, No. 9, p. 10.
[453] Ibid.
[454] Ibid.
[455] Opinion Of Advocate General Szpunar delivered on 10 January 2019, para. 27.

options for applying the right to be forgotten, but rather at finding the most acceptable balance between them. This can already be seen in the EU case law, in particular in the same case of *Glawischnig-Piesczek v. Facebook*.

The protection of the digital rights exposes a tension between efforts of states to impose their own standards outside their borders and aspirations to claim sovereign control over data and information. This tension exposes the risk of a fragmentation of the digital world. Although it is obvious that such a tension in the framework of these opposite tendencies, as a rule, is mostly growing. And as the Court's case law shows, it tries to offer judgments that will vary between these two extremes, as in *Google v. CNIL* and *Glawischnig-Piesczek v. Facebook*. The *CNIL* case defines the local application of law and allows for further recognition of the global application of EU law and the right to be forgotten in particular. But if in the *CNIL* case the Court limited itself only to stating that in certain cases such a global application is permissible, then in the *Glawischnig-Piesczek* case the Court suggested such an application as the main solution to the questions raised in the preliminary request.

So, the *Google v. CNIL* judgment cannot be considered as a reduction in the level of data protection and a refusal to globally application of right to be forgotten. On the contrary, it allows for the further application of the global application of the right to be forgotten and becomes a step towards adapting the EU data protection law to the reality of the Internet. This is an attempt to develop progressive case law to protect human rights in the digital age.

The right to be forgotten is increasingly faced with the issue of jurisdictional boundaries, and the *Google v. CNIL* case does not exhaust this issue and does not reduce the likelihood of further litigation regarding the scope of the right to be forgotten.

In addition to setting limits on the territorial scope of the right to be forgotten, the *CNIL* case is significant in that it paved the way for global coverage. From the EU's point of view, extraterritorial enforcement of the EU's digital rights, in particular the right to be forgotten, is seen as a way guaranteeing full protection of human rights. Nevertheless, developing rules for the protection of digital privacy in the context of balancing these two approaches, rather than opting for one of them, is the best way forward to ensure that privacy remains a protected right, even in the digital age. This position is expressed by the solution under consideration. Therefore, the interpretation of the judgment of the *CNIL* case as a territorial restriction of the right to be forgotten cannot be considered correct. Rather, it was the first attempt to balance the local and global application of the right to be forgotten.

7 Conclusion

With the development of information and communication technologies and the expansion of the collection and processing of personal information, the protection of personal privacy and confidentiality has gained new meaning and has become necessary to develop new legal mechanisms to prevent new privacy risks. Digital technologies, including databases, Internet, etc., call for further evolution of privacy rights, both conceptually and legislatively. Legal issues regarding privacy have increasingly begun to be considered in the context of issues of access, control and protection of information in the online environment. Data protection has become one of the main approaches to regulating the protection of privacy and confidentiality, including in EU law, where the right to data protection has been elevated to the rank of fundamental.

After the *Google Spain* case, the right to data protection gained momentum, but in a very narrow aspect – as the right to demand that information is no longer provided to the general public by excluding the list from the results returned by a search performed by reference to the name of the data subject. Nevertheless, the provisions of the case raised more questions than answers, primarily about the legality, legal nature and scope of application of this right. After the adoption of the GDPR, the issues also did not receive a solution. The analysis of the GDPR itself showed that there is no general right to disclose personal information, the right can be used only in these limited situations, and the issue of applying this right is decided by corporations with an economic interest. In addition, the right to be forgotten acquires the characteristics of an instrument of market regulation and redistribution of powers between data subjects and data processors between private entities. The subsequent judicial practice of the EU does not form a common vision and accuracy in the development and implementation of the legal framework of the right to be forgotten, however, it forms the scope of the right to be forgotten case-by-case.

In order to expand the scope of the right to be forgotten and use it as a mechanism to counteract the risks of the Internet, it seems more effective to substantiate the right through the right to personal identity, which will provide an opportunity for the protection and post-mortem confidentiality. I suppose that the right to be forgotten can be defined as a legal requirement that allows the erasure of "digital traces" left on the Internet in order to protect an individual, his dignity, reputation, privacy and identity in the online world. Such a definition makes it possible to include both an individual and a possible collective requirement for such erasure.

One of the problematic aspects of the right to be forgotten is the balancing act between the right to be forgotten and the right to express an opinion. In this context, the difference between the regulation of the right to be forgotten in EU law and in the case law of the ECtHR is more prominently emphasized. Firstly, if the CJEU explicitly indicates the priority of the right to be forgotten, with some exceptions, the ECtHR has not yet explicitly approved the priority of the right to be forgotten after balancing through six *Axel Springer's* criteria, nevertheless giving some flexibility in their acceptance, which allows us to see recognition of the priority of the right to be forgotten. Here one can see the moment of some influence of the EU judicial practice on the formation of the ECtHR's approach. Nevertheless, time will tell whether this approach will be strengthened in the judicial practice of the ECtHR, established in the cases of *Hurbain v. Belgium* and *Biancardi v. Italy*.

At the same time, it should be pointed out that the right to be forgotten in the judicial practice of the CJEU and the ECtHR have different meanings. The ECtHR considers the right to be forgotten in the context of the right to privacy and includes control over personal data, claims to confidentiality and reputation, damage caused to the data subject, the passage of time, public interest in the dissemination of information, contextualization of news and the role that online information plays. Media archives and search engines are also elements that need to be weighed and compared when balancing the rights in question. The CJEU is indifferent to this damage, revolving its reasoning around the legality of data processing. In addition, unlike the CJEU, the ECtHR expands the scope of the right to be forgotten, systematically extending the right to be forgotten to the press. The ECtHR argues that it is legitimate to require a news organization, rather than a search engine, to de-index personal information, provided that this information is stored in its internal paper and digital archives, and the public can access it directly for complete information. These differences of opinion do not contribute to clarifying the nature of the right to be forgotten and the conditions for its recognition, and may lead to uncertainty about the interpretation of European legal systems and contribute to concerns about the scope of the right to be forgotten. Due to the fact that there is no single standard for the protection of fundamental rights in Europe, the right to be forgotten will continue to be an uncertain right, the balancing of which has been transferred to a greater extent to private subjects and the national legislator.

The potential expansion of the concept of personal data in the current EU regulatory framework is due, in particular, to the possibility of an overly broad interpretation of the requirement of identifiability, the breadth of the term "relating to", the dichotomy of identifiability/anonymity. The CJEU is trying to provide sufficient tools for the interpretation

of these terms in order to guarantee the flexibility of the concept of personal data to ensure the effective exercise of the right to data protection, which cannot be fully ensured if a narrow interpretation is applied, in which some data will not be protected. At the same time, the potential width of the "*refering to*" link is limited by its interaction with the identification requirement, and the extensive effect of the identifiability requirement can be curbed by applying a variety of criteria developed for the "reasonable probability" test, not only to the means that can be used to identify the data subject, but also to the persons to whom these means may be available, and their relationship with the controller. Nevertheless, the breadth of the concept of "personal data" makes it difficult to apply the right to be forgotten. Assessing whether the data is "personal data" is only the first step in assessing the applicability of the right to be forgotten. The right to be forgotten contributes significantly to the achievement of the data protection objectives set out in the GDPR and in the judicial practice of the EU. This ensures that the law can be applied to unforeseen contexts and/or data. A functional approach and a detailed interpretation of the scope of the GDPR are crucial for the effective and proportionate application of the right to be forgotten.

In the context of the prospects and challenges of the development of the right to be forgotten in the EU, special attention should be paid to the need to develop mechanisms to protect the *ipse* identity. The right to be forgotten has the potential to become one of the mechanisms for protecting such an identity. Considering the right to be forgotten in the key of personal identity may help to find a new balance of interests. I conclude that the scope of the right to be forgotten should be expanded and the right to personal identity and human dignity should be considered as a justification. This approach will make it possible to extend this right to the sphere of protection of *post-mortem* privacy as well and further increase the effectiveness of human protection in the digital sphere. Currently, there is a situation where neither primary nor secondary EU legislation, nor the ECHR, nor the case law of both European Supranational Courts explicitly provide for posthumous data protection in the EU. Death, being not only the ultimate boundary of human biological life, also means the end of a living subject with his/her long-term goals and hopes for his/her own achievements and personal enjoyment. As a result, in many cases, the issue of *post-mortem* data protection remains at the unlimited discretion of the Internet service providers and social networks themselves, which provide a postmortem data protection policy convenient for them, taking into account their business needs. However, the EU legislator should try to create such a unified mechanism for posthumous data protection and the policy of EU legislators regarding discretion should be changed.

The issues of territorial application of the right to be forgotten are considered, in particular in the context of the possibility of its global spread. Having reviewed the judicial practice of the CJEU, I come to the conclusion that the CJEU is faced not with a choice between local and global application of the right to be forgotten, but rather with the need to develop criteria that would help regulate the application of EU data protection legislation outside the borders of the EU.

I state that at the moment, the protection of the applicant's privacy and reputation in court proceedings is not effective enough. Practice shows that applicants who have applied to the CJEU and the ECtHR for the removal of unwanted information often become even more connected with such information in the digital world. At the same time, the Courts must clearly understand that the relationship between privacy and freedom of expression and information has always been and remains a painful topic for human rights law in general. For the effective coexistence of these two fundamental rights, it is necessary that the Courts carefully describe the factual circumstances of the cases in their judgments concerning the exercise of the right to be forgotten. Otherwise, we will witness new cases of the Streisand effect, which will leave their negative imprint on the further development of the case law of European Supranational Courts.

I believe that the best solution on the part of the courts would be to adhere to the policy of the "golden mean" when describing the actual circumstances in judgments. That is, on the one hand, the Courts must ensure the protection of the applicants' privacy and confidentiality so that it is not possible to identify the applicants and their data, and, on the other hand, the Courts must indicate the factual circumstances in such a way that it is clear from which facts the Courts proceed and develop their legal arguments. It is possible to ensure these two steps at the same time: one does not contradict the other, otherwise it would be impossible to simultaneously protect both the right to privacy and freedom of expression and information, as the EU protects in the CFR, and the Council of Europe protects in the ECHR.

I believe that the solution to the problem lies in finding a proportionate and adequate balance between the privacy and confidentiality of the applicants and the description of the main factual circumstances of the case. The practice that I have indicated above should be applied in any case where the subject of the case is the right to be forgotten. Moreover, this practice should be applied regardless of the outcome of the case. This will help to avoid future cases of the "Streisand effect" and at the same time ensure both respect for human privacy by the Courts and prevent abuse of this right (for example, as a means of PR). Thus, the Courts

will arouse even greater confidence in the eyes of applicants as guarantors of human rights protection and will not make them afraid to defend their rights in the courts.

Bibliography and resources

Monographs, scholarly books and proceedings, scientific articles, papers and chapters

ACQUISTI, Alessandro, et al. Privacy and human behavior in the age of information. Science, Vol. 347, No. 6221, 2015, p. 510.

AHMED, Farhaan Uddin. Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm. Computer and Telecommunications Law Review, Vol. 21, No. 6, 2015, pp. 175-185.

ALBRECHT, Jan Philip. Die EU-Datenschutzgrundverordnung rettet die informationelle Selbstbestimmung! Zeitschrift für Datenschutz, 2013, p. 587.

ALESSI, Stefania. Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation. Emory International Law Review, 2017, Vol. 32, no. 1, pp. 145–171.

ALLEGRI, Maria Romana. The Right to be Forgotten in the Digital Age. In COMUNELLO, Francesca et al. (eds.) What People Leave Behind. Frontiers in Sociology and Social Research. Springer, Cham, Vol 7., 2022, pp. 237-251.

ALLEN, Anita, L. Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm Commentary. Connecticut Law Review, 2000, vol. 32, No. 3, p. 867.

ANDRADE, Norberto Nuno Gomes de. Oblivion: The Right to Be Different from Oneself - Reproposing the Right to Be Forgotten. Revista de Internet, Derecho y Política. No. 13, pp. 122-137.

ANDRADE, Norberto Nuno Gomes de. Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization. In GUTWIRTH, Serge, et. al. (eds.). Computers, Privacy and Data Protection: An Element of Choice. Springer, 2011, pp. 65-97.

ARISTOTLE, Nicomachean Ethics II.1

ATWATER, Justin. Who owns E-mail? Do you have the right to decide the disposition of your private digital life? Utah Law Review. 2006. Vol. 2006, No. 2, pp. 397-418.

BAMBERGER, Kenneth A., MULLIGAN, Deirdre K.. Privacy in Europe: Initial Data on Governance Choices and Corporate Practices. The George Washington Law Review, Vol. 81, 2013, p. 1539.

BEAUMONT, Paul. Striking a Balance: Hate Speech, Freedom of Expression and Non-Discrimination. International and Comparative Law Quarterly. 1994, Vol. 43 No. 2, pp. 476-478.

BENN, Stanley I. Privacy, freedom, and respect for persons. In SCHOEMAN, Ferdinand David (ed.) Philosophical Dimensions of Privacy: An Anthology, Cambridge: Cambridge University Press, 1st edition, pp. 223–244.

BERNAL, Paul A.. A Right to Delete?. European Journal of Law and Technology, 2011, Vol. 2, No.2, pp. 1-18.

BLANCHETTE, Jean-François, JOHNSON, Deborah G. Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness. The Information Society, Vol. 18, No. 1, 2002, pp. 33–45.

BOK, Sissela. Secrets: On the Ethics of Concealment and Revelation, Pantheon. New York: Oxford University Press, 1983, 332 p.

BORKOWSKI, Susan, DECEW, Judith Wagner, In Pursuit of Privacy: Law, Ethics and the Rise of Technology. Teaching Business Ethics, 1999, vol. 3, No. 4, pp. 402–406.

BOURDELOIE, Hélène. Usages des dispositifs socionumériques et communication avec les morts. Questions de communication. Vol. 28, 2015, p. 103.

BRUNTON Finn, NISSENBAUM, Helen, Obfuscation: A User's Guide for Privacy and Protest, Cambridge, MA: MIT Press. 2015, 49 p.

BUITELAAR, Jan. Post-mortem privacy and informational self-determination.Ethics and Information Technology, Vol. 19, No. 2, 2017, pp. 129-142.

BUITELAAR, Marjo 'Discovering a different me': Discursive positioning in life story telling over time. Women's Studies International Forum, 2014. Vol. 43, pp. 30-37.

CANNATACI, Joseph A., et. al. Privacy, free expression and transparency: Redefining their new boundaries in the digital age. Unesco Publishing, 2016, 142 p.

CARROLL, Evan, ROMANO, John. Your digital afterlife: When Facebook, Flickr and Twitter are your estate, what's your Legacy? Berkeley, CA: New Riders, 2011, 203 p.

CARTER, Edward L. The Right To Be Forgotten. Oxford Research Encyclopedia of Communication, Oxford: Oxford University Press, 2016. 3 p.

CAYOL, Amandine. Avant La Naissance et Après La Mort: L'être Humain, Une Chose Digne de Respect. Cahiers de La Recherche Sur Les Droits Fondamentaux, No. 9, 2011, p. 124.

CIESLIK, Katarzyna, MARGÓCSY Dániel. Datafication, Power and Control in Development: A Historical Perspective on the Perils and Longevity of Data. Progress in Development Studies, Vol. 22, No. 4, 2022, pp. 352–373.

CLARKE, Roger. The Digital Persona and Its Application to Data Surveillance. The Information Society, Vol. 10, No. 2, 1994, pp. 77–92.

CROCKETT, May. The Internet (Never) Forgets. Science and technology Law Review. 2017, Vol. 12, No. 2., pp. 151–181.

CULIK, Nicolai, DÖPKE, Christian. About Forgetting and Being Forgotten. In HOEREN, Thomas, KOLANY-RAISER, Barbara (eds.) Big Data in Contex. Springer International Publishing, 2018, pp. 21–27.

DALLA CORTE, Lorenzo. Safeguarding data protection in an open data world: On the idea of balancing open data and data protection in the development of the smart city environment and data protection in the development of the smart city environment. Tilburg: Tilburg University, 2020, 125 p.

DASKAL, Jennifer. SPEECH ACROSS BORDERS. Virginia Law Review, 2019, Vol. 105, No. 8, pp. 1605–1666.

DE ANDRADE, Norberto Nuno Gomes. The right to personal identity in the information age: a reappraisal of a lost right. Florence: European University Institute, Ph.D. Thesis, Italy, 2012.

DE HERT, Paul, PAPAKONSTANTINOU, Vagelis. Google Spain: Addressing Critiques and Misunderstandings One Year Later. Maastricht Journal of European and Comparative Law, Vol. 22, No. 4, 2015, pp. 624–638.

DE TERWANGNE, Cecile. Internet privacy and the right to be forgotten/right to oblivion. Revista de Internet, derecho y politica, 2012, Vol. 13, pp. 31-43.

DECEW, Judith Wagner, In Pursuit of Privacy: Law, Ethics, and the Rise of Technology, Ithaca, New York: Cornell University Press, 1997, 199 p.

DEVRIES, Will Thomas. Protecting Privacy in the Digital Age. Berkeley Technology Law Journal. 2003, Vol. 18, p. 283.

DIGGELMANN, Oliver, CLEIS, Maria Nicole. How the Right to Privacy Became a Human Right, Human Rights Law Review, 2014, vol. 14, No. 3, pp. 441–458.

EDWARDS, Lilian, HARBINJA, Edina, Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World. Cardozo Arts & Entertainment Law Journal, Vol. 32, No. 1, 2013, pp. 83-129.

FABBRINI, Federico, CELESTE, Edoardo. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. German Law Journal. Vol. 21, No. 1, 2020. pp. 55-65.

FAISAL, Kamrul. Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions. SECURITY AND PRIVACY, 2021, Vol. 4, no. 4, p. 157

FINCK, Michèle, PALLAS, Frank. They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR. International Data Privacy Law, 2020, Vol. 10, No. 1, pp. 11–36.

FINOCCHIARO, Giusella. Il diritto all'oblio nel quadro dei diritti della personalità. Il Diritto Dell'informazione e Dell'informatica, Vol. 4 No. 5, 2014, pp. 591-604;

FLORIDI, Luciano, TADDEO, Mariarosaria, What is Data Ethics? Philosophical Transactions of the Royal Society A, Vol. 374, No. 2083, 2016, p. 1592.

FLORIDI, Luciano. The fourth revolution: how the infosphere is reshaping human reality. Oxford: Oxford University Press. 2014, 248 p.

FLORIDI, Luciano. The Information Society and Its Philosophy: Introduction to the Special Issue on The Philosophy of Information, Its Nature, and Future Developments. The Information Society, Vol. 25, No. 3, 2009, pp. 153–158;

FLORIDI, Luciano. The informational nature of personal identity. Minds and Machines, 2011, Vol. 21, No. 4, pp. 549-566.

FLORIDI, Luciano. The ontological interpretation of informational privacy. Ethics and Information Technology, 2005, Vol. 7, No. 4, pp. 185-200.

FRIED, Charles. Privacy. The Yale Law Journal, 1968, vol. 77, No. 3, pp. 475-493.

FROSIO, Giancarlo F. The Death of 'No Monitoring Obligations': A Story of Untameable Monsters, Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 8, No. 3, 2017, p. 335.

FUSTER, Gloria González, GELLERT, Raphaël. The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right. International Review of Law, Computers amd Technology. 2012, Vol. 26, No. 1, pp. 73–82.

GAVISON, Ruth. Privacy and the Limits of Law. Yale Law Journal. 1980, Vol. 89, No. 3, p. 428.

GLOBOCNIK, Jure. The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17). GRUR International. Vol. 69, No. 4, 2020, pp. 380-388.

GSTREIN, Oskar Josef. Right to be forgotten: European data imperialism, national privilege, or universal human right? Review of European Administrative Law (REALaw), 2020, Vol. 1, pp. 136-139.

GSTREIN, Oskar; BEAULIEU Anne. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philos. Technol, 2022, vol. 35, No. 3, pp. 43–44.

HAMUĽÁK, Ondrej, et al. The Global Reach of the Right to be Forgotten through the Lenses of the Court of Justice of the European Union. Czech Yearbook of Public and Private International Law, 2021, Vol. 12, pp. 196-211.

HAMUĽÁK, Ondrej; KOCHARYAN, Hovsep; KERIKMÄE, Tanel. The Contemporary Issues of Post-Mortem Personal Data Protection in the EU after GDPR entering into Force. In: Czech Yearbook of Public and Private International Law, 2020, vol.11, pp. 225−238.

HAMUĽÁK, Ondrej; KOCHARYAN, Hovsep; KERIKMÄE, Tanel; MUURSEPP, Peeter. Legal Person or Agenthood of Artificial Intelligence Technologies. Acta Baltica Historiae et Philosophiae Scientiarum, 2020, vol.8 (2), pp. 73−92.

HARGITTAI, Eszter, MARWICK, Alice. 'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy. International Journal of Communication, Vol. 10, 2016, pp. 3737–3757.

HILL, Richard. Internet Governance, Multi-Stakeholder Models, and the IANA Transition: Shining Example or Dark Side? Journal of Cyber Policy, Vol. 1, No. 2, 2016, pp. 176-197.

HOOFNAGLE, Chris Jay et. al. The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, 2019, vol. 28 No. 1, pp. 69-72.

HUCKVALE, Kit, et al. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. JAMA Network Open, Vol. 2, No. 4, 2019, p. 10.

JANEČEK, Václav. Ownership of Personal Data in the Internet of Things. Computer Law and Security Review, 2018, Vol. 34, No. 5, pp. 1039-1052.

JONES, Meg Leta, AUSLOOS, Jef. The Right to Be Forgotten Across the Pond. Journal of Information Policy, Vol. 3, 2013, pp. 1-23.

JONES, Meg Leta. Ctrl + Z: The right to be forgotten. New York: New York University Press. 2016, 75 p.

JOSEPH, Sarah, CASTAN, Melissa. The International Covenant on Civil and Political Rights: Cases, Materials and Commentary. Oxford: Oxford University Press, 2013, 1042 p.

JUSTIN, Clark et al. Content and Conduct: How English Wikipedia Moderates Harmful Speech. Harvard University, Berkman Klein Center for Internet & Society, 2019, 76 p.

KHATCHATOUROV, Armen. Digital Regimes of Identity Management: From the Exercise of Privacy to Modulation of the Self. In KHATCHATOUROV, Armen. et al. (eds.). Digital Identities in Tension: Between Autonomy and Control, London: ISTE Editions, 2019, p. 30.

KOCHARYAN, Hovsep; HAMUĽÁK, Ondrej; KISS, Lilla Nóra, GABRIS, Tomáš. "This Content is not Available in Your Country". A General Summary on Geo-Blocking in and outside the European Union. International and Comparative Law Review, 2020, Vol. 21 (1), pp. 153−183.

KOCHARYAN, Hovsep; HAMUĽÁK, Ondrej; VARDANYAN, Lusine, KERIKMÄE, Tanel. Critical Views on the Right to be Forgotten after the Entry into Force of the GDPR: Is it Able to Effectively Ensure our Privacy? *International and Comparative Law Review*, 2021, vol. 21 (2), pp. 96−115.

KOCHARYAN, Hovsep; HAMUĽÁK, Ondrej; VARDANYAN, Lusine. The Global Reach of the Right to be Forgotten through the Lenses of the Court of Justice of the European Union. Czech Yearbook of Public & Private International Law, 2021, vol. 11, pp. 196−211.

KOCHARYAN, Hovsep; HAMUĽÁK, Ondrej; VARDANYAN, Lusine. The Right to be Remembered?: The Contemporary Challenges of the "Streisand Effect" in t*he European Judicial Reality. International and Comparative Law Review*, vol.22, no.2, 2022, pp.105-120.

KOCHARYAN, Hovsep; STEHLIK, Vaclav; VARDANYAN, Lusine. Digital integrity: the foundation for digital rights and the new manifestation of human dignity. *TalTech Journal of European Studies*, 2022, vol. 12, No. 1 (35), pp.160-185.

KOCHARYAN, Hovsep; VARDANYAN, Lusine. The right to data protection in the light of personality rights: does it prevent the emergence of data ownership? *Journal of Ethics and Legal Technologies*, 2022, 4(1), pp.105-120.

KOCHARYAN, Hovsep; VARDANYAN, Lusine. Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: main obstacles and challenges. *European Studies*, 2022, 9(2), pp. 110-132.

KOCHARYAN, Hovsep; VARDANYAN, Lusine. The GDPR and the DGA proposal: are they in controversial relationship? In: *European Studies. The Review of European Law, Economics and Politics*, 2022, vol. 9, issue 1, pp. 91-109.

KOOPS, Bert-Jaap. Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to Be Forgotten" in the Big Data practice. SCRIPTed., Vol. 8, No. 3, 2011., pp. 229-256.

KUCZERAWY, Aleksandra, AUSLOOS, Jef. From notice-and-takedown to notice-and-delist: Implementing Google Spain. Colorado Technology Law Journal, 2016, Vol. 14, No. 2, pp. 219-258.

KÜHLING, Jürgen, RAAB, Johannes. Einführung, In KÜHLING, Jürgen, BUCHNER, Benedikt (eds.), Datenschutz-Grundverordnung BDSG Kommentar, 3rd edition, C.H. Beck, 2020, 26 p..

KUNER, Christopher. The Internet and the Global Reach of EU Law. In CREMONA, Marise, SCOTT, Joanne (eds.). EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law. Oxford: Oxford University Press, 2019, pp. 112–145.

KUNER, Christopher. The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges. In HESS, Burkhard, MARIOTTINI, Cristina M. (eds.). Protecting Privacy in Private International and Procedural Law and by Data Protection: European and American Developments. Baden-Baden: Nomos; Ashgate, 2015, pp. 19-55.

KWASNY, Tatjana, et. al. Towards reduced meat consumption: A systematic literature review of intervention effectiveness, 2001–2019. Appetite, 2022, vol. 168, 17 p.

KWET, Michael. 'Digital Colonialism: US Empire and the New Imperialism in the Global South'. Race and Class, Vol. 60, No., 2019, pp. 3–26.

LEE, Edward. The Right to Be Forgotten v. Free Speech. A Journal of Law and Policy for the Information Society. Vol. 12, No. 1. 2015, p.110.

LYNSKEY, Orla. Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. Modern Law Review 522. Vol. 78 No. 3., 2015, pp. 522-534.

LYNSKEY, Orla. The Foundations of EU Data Protection Law. Oxford: Oxford University Press. 2015. 336 p.

MACH, Martin. Streisand Effect in the Context of the Right to be Forgotten. European Studies – the Review of European law, Economics and Politics. 2022, vol. 9, no. 1, pp. 110–121.

MALGIERI, Gianclaudio. 'R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions'. In LEENES, Ronald et. al (eds.). Data Protection and Privacy: The Internet of Bodies. 2018, Hart Publishing, pp. 300-320.

MALGIERI, Gianclaudio. Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data. Privacy in Germany, Vol. 2016, No. 4, 2016, p. 133; DE FRANCESCHI, Alberto; LEHMANN, Michael. Data as a Tradeable Commodity and New Measures for their Protection, The Italian Law Journal, Vol. 1, No. 1, 2016. pp. 51-52.

MANTELERO, Alessandro. The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'. Computer Law and Security Review. 2013, Vol. 29, No. 3, pp. 229–235.

MARSHALL, Jill. Personal Freedom through Human Rights Law?: Autonomy, Identity and Integrity

MAYER-SCHÖNBERGER, Viktor. Delete: The virtue of forgetting in the digital age. Princeton: Princeton University Press, 2009, 272 p.

MAZÚR, Ján, PATKYOVÁ, Mária T. Regulatory Approaches to Facebook and Other Social Media Platforms: Towards Platforms Design Accountability. Masaryk University Journal of Law and Technology, 2019, Vol. 13, No. 2, pp. 219-241.

MCCARTHY, Hugh, COX, Arthur. Expanding the GDPR's journalism exemption - is all the world a stage? Privacy and Data Protection. 2019. Vol. 14, No. 9, p. 10.

NARAYANAN, Arvind, SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiable Information". Communications of the ACM, 2010, Vol. 53, No. 6, p. 24.

NISSENBAUM, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford: Stanford University Press, 2009. 304, p.

NURULLAEV, Ruslan. Right to Be Forgotten in the European Union and Russia: Comparison and Criticism. Pravo. Zhurnal Vysshey shkoly ekonomiki. 2015. No. 3. p. 181-193.

OKORO, Egoyibo Lorrita. Death and Personal Data in the Age of Social Media. Tilburg: Tilburg University. LLM Law and Technology, 2018, 48 p.

OREG, Elad. Right to Information Identity, John Marshall Journal of Computer & Information Law, 2012, Vol. 29., No. 4, pp. 539-592.

OVČAK KOS, Maja. The right to be forgotten and the media. Lexonomica. Vol. 11, No. 2, 2019, pp. 195–212.

OWINGS, Lisa. The Right To Be Forgotten. Akron Intellectual Property Journal. Vol. 9, No. 1, 2015. pp. 45-82.

PADOVA, Yann. Is the right to be forgotten a universal, regional, or 'glocal' right?, International Data Privacy Law, 2019, Vol. 0, No. 0, pp. 1-15

PAGALLO, Ugo, DURANTE, Massimo. Human rights and the right to be forgotten. In SUSI, Mart (ed.) Human Rights, Digital Society and the Law: A Research Companion. 1st edition, Routledge, 2019, 412 p., p. 21

PAPACHARISSI, Zizi, GIBSON, Paige L.. Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites., In TREPTE, Sabine, REINECKE, Leonard (eds.). Privacy Online. Springer Berlin Heidelberg, 2011, pp. 75–89

PAVELEK, Ondřej, ZAJÍČKOVÁ, Drahomira. Personal Data Protection in the Decision-Making of the CJEU Before and After the Lisbon Treaty. Baltic Journal of European Studies. 2021, Vol. 11, No. 2, p. 167.

PEUCKER, Enrico. The "right to be forgotten" in Germany. In: TAMBU, Olivia (ed.). The right to be forgotten in Europe and beyond/ The right to love in Europe and beyond. 2018, Luxembourg: Blogdroiteuropéen, Open access collection, 34-40 p.

PINO, Giorgio. Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali. In PANETTA, Rocco (ed). Libera circolazione e protezione dei dati personali, 2006, MILANO: Giuffre', 275-321 p.

PINO, Giorgio. l'identità personale. In RODOTÀ, Stefano, TALLACCHINI, Mariachiara (eds.), Trattato di biodiritto, 2010, vol. I, Ambito e fonti del biodiritto. Milano: Giuffrè, 297-321 p.

POLITOU, Eugenia, et. at.: Backups and the right to be forgotten in the GDPR: An uneasy relationship. Computer Law & Security Review. 2018, Vol. 34., No. 6., pp. 1247-1257.

POSNER, Richard A. Economic Analysis of Law, Economic Analysis of Law, 5th edition, Aspen, Vol. 46, 660-663 pp.

PURTOVA, Nadezhda. Do property rights in personal data make sense after the big data turn: Individual control and transparency. Journal of Law and Economic Regulation, Vol. 10, No. 2, 2017, pp. 64–78.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology. Vol. 10, No. 1, 2018, pp. 40-81

RENGEL, Alexandra. Privacy-Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights. Intercultural Human Rights Law Review. 2013, Vol. 8, pp. 177 – 230.

RESTA, Giorgio. La "morte" digitale. Milano: Giuffrè Editore, 2014, 892 p.

RHÉA, Eddé. Le droit: un outil de régulation du cyberespace? Le cas du droit à l'oubli numérique. L'Homme & la Société. 2018, Vol. 1, No. 206, p. 69.

ROBERTS, Huw. Informational Privacy with Chinese Characteristics. In MÖKANDER, Jakob, ZIOSI, Marta (eds.). The 2021 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook. Springer, Cham., 2022, pp. 9-23.

ROSEN, Jeffrey. The right to be forgotten. Stanford Law Review Online, 2012, Vol. 64, pp. 88–92.

ROUVROY, Antoinette, POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development. In GUTWIRTH, Serge et al. (eds.), Reinventing Data Protection. Springer, 2009, 68 p.

SCANLON, Thomas. Thomson on Privacy, Philosophy and Public Affairs, 1975, vol. 4, No. 4, pp. 315-322.

SCHMIDT, Bernd, Art. 1 DSGVO. In TAEGER, Jürgen, GABEL, Detlev (eds.), DSGVO BDSG, 3rd edition, Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, 2019, 25 p.;

SCHÜNEMANN, Wolf J., BAUMANN, Max-Otto. Privacy, data protection and cybersecurity in Europe. New York, NY: Springer International Publishing, 2017, 145 p.

SCHWARTZ, Paul M. Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology. William and Mary Law Review, Vol. 53, No. 2, 2011, p. 368;

SCHWARTZ, Paul M., SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. New York University Law Review, 2011, Vol. 86, p. 1814.

SELBST, Andrew D. Contextual Expectations of Privacy. Cardozo Law Review, 2013, Vol. 35, No. 2, pp. 699–705.

SMOLENSKY, Kirsten Rabe. Rights of the dead. Hofstra Law Review. 2009, Vol. 37, No. 3, pp. 763-803.

SOLOVE, Daniel J. The Digital Person: Technology and Privacy in the Information Age. New York University Press, 2004, 296 p.

SPERLING, Daniel. Posthumous Interests. Cambridge: Cambridge University Press, 2008, 304 p.

STONE SWEET, Alec. The European Court of Justice and the judicialization of EU governance. Living Reviews in European Governance. 2010, p. 1.

SULLIVAN, Clare, Privacy or Identity? International Journal of Intellectual Property Management Vol. 2, no. No. 3, 2008, p. 297.

SULLIVAN, Clare. Digital Identity – the Legal Person? Computer Law and Security Review Vol. 25, No. 3, 2009, pp. 227-236.

SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation. International Data Privacy Law. Vol. 5, No. 4, 2015, p 230.

TAMÒ, Aurelia, DAMIAN, George. Oblivion, Erasure and Forgetting in the Digital Age. Journal of Intellectual Property. Information Technology and E-Commerce Law. Vol. 71. No. 2, 2014, p. 74.

TAYLOR, Mistale. Google Spain Revisited: The Misunderstood Implementation of a Landmark Decision and How Public International Law Could Offer Guidance. European Data Protection Law Review. 2017, Vol. 3, No. 2, pp.195-208.

TAYLOR, Mistale. Reasonableness in its reasoning: How the European Union can mitigate problematic extraterritoriality on a de-territorialised internet. Questions of International Law, 2019, Vol. 62, pp. 35-53.

TAYLOR, Mark. Genetic Data and the Law: A Critical Perspective on Privacy Protection, Cambridge: Cambridge University Press, 2012, 140 p.;

THOMSON, Judith Jarvis. The Right to Privacy. Philosophy and Public Affairs, Princeton, N.J: Princeton University Press, 1975, vol. 4, No. 4. pp. 295-314.

TIROSH, Noam. 'Reconsidering the "Right to Be Forgotten' – Memory Rights and the Right to Memory in the New Media Era. Media, Culture & Society, Vol. 39, No. 5, 2017, pp. 644–660.

TOROP, Henri. Õigus olla unustatud - kas rahvusvaheliselt tunnustatud inimõigus? Avaliku õiguse osakond. Tartu: Magistritöö, 2018. 98 p.

URGESSA, Worku Gedefa. The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging 'Data' as Exclusively Informational, JIPITEC, Vol. 96, No. 7, 2016, p. 1.

URGESSA, Worku Gedefa. The Protective Capacity of the Criterion of Identifiability under EU Data Protection Law. European Data Protection Law Review, Vol. 2, 2016, p. 521.

VAN DER SLOOT, Bart. Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR. In TAYLOR, Linnet, FLORIDI, Luciano, VAN DER SLOOT, Bart (eds.), Group Privacy: New Challenges of Data Technologies. Springer International Publishing, 2017, pp. 197–224.

VARDANYAN, Lusine, et. al. Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. TalTech Journal of European Studies, Vol.12, No.1, 2022, pp.159-185.

VARDANYAN, Lusine; HAMUĽÁK, Ondrej; KOCHARYAN, Hovsep; KERIKMÄE, Tanel. The Digital Sovereignty of the EU – Marking Borders in the Digital World? In: *Digital development of the European Union, Springer International Publishing*, 2023, pp. 196–211.

VEALE, Michael. Sovereignty, privacy and contact tracing protocols. Data Justice and COVID-19: Global Perspectives. In: TAYLOR, Linnet et. al. (eds.) Data Justice and COVID-19: Global Perspectives. London: Meatspace Press. 2020. pp. 34–39.

VELIZ, Carissa. Privacy is Power: Why and How You Should Take Back Control of Your Data, London: Bantam Press. 2021, 224 p.

WARREN, Samuel D.; BRANDEIS, Louis D. Right to privacy. Harvard Law Review, 1890, vol. 4, No. 5., pp. 193-220.

WEBER, Rolf. The Right to Be Forgotten: More Than a Pandora's Box? JIPITEC, 2011, Vol. 120, pp.120-130.

WECHSLER, Simon. The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten. Columbia Journal of Law and Social Problems, 2015, Vol. 49, pp. 135-165.

WESTIN, Alan F., Privacy and Freedom, New York: Atheneum, 1967, 487 p.

WINTER, Stephen. Against posthumous rights. Journal of Applied Philosophy, 2010, Vol. 27, No. 2, pp. 186-199;

ZALNIERIUTE, Monika. Google LLC v. Commission nationale de l'informatique et des libertés (CNIL). *American Journal of International Law*, 2020, Vol. 114., No. 2, pp. 261 – 267.

ZHAO, Bo. Posthumous Defamation and Posthumous Privacy Cases in the Digital Age. Savannah Law Review, Vol. 3, No. 1, 2016, pp. 15-35.

ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

Electronic [online] articles and contributions

Access Now. Position paper: understanding the right to be forgotten globally. AccessNow. [online]. September 2016, [cit. on. 25th December 2023]. Accessible at: <https://www.accessnow.org/wp-content/uploads/2017/09/RTBF_Sep_2016.pdf>.

ALKIVIADOU, Natalie. Hate Speech by Proxy: Sanchez v France and the Dwindling Protection of Freedom of Expression. OpinioJuris [online]. 14th December 2021. [cit. on. 25th December 2023]. Accessible at: <https://opiniojuris.org/2021/12/14/hate-speech-by-proxy-sanchez-v-france-and-the-dwindling-protection-of-freedom-of-expression/>.

Article 19. The Right to be Forgotten: Remembering Freedom of Expression. [online]. 2016. [cit. on. 25th December, 2023]. Accessible at: <https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf>.

BARLOW, John Perry. A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation [online]. 8th February 1996. [cit. on. 25th December 2023]. Accessible at: <https://www.eff.org/cyberspace-independence>.

BERNAL, Paul A. The Right to Online Identity. SSRN Electronic Journal [online]. September 2012. [cit. on 25th December 2023]. Accessible at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143138>.;

BOWCOTT, Owen. "Right to be forgotten" could threaten global free speech, say NGOs'. The Guardian [Online]. 9th September 2018. [cit. on. 25 December 2023]. Accessible at: <https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos>.

CASTELLANO, Pere Simón. The Right to Be Forgotten under European Law: a Constitutional Debate. Lex Electronica. Vol. 16, No. 1 [online]. [cit. 2019-09-22]. Accessible at: <www.lex-electronica.org/docs/articles_300.pdf>.

CHARLES, Arther. Tech giants may be huge, but nothing matches big data [online]. Guardian. 23th August 2013. [cit. on. 25th December 2023]. Accessible at: <http://www.theguardian.com/technology/2013/aug/23/tech-giants-data>

COWBURN, Pam. Google win in right to be forgotten case is victory for global freedom of expression. Article 19 [online]. 24th September 2019. [cit. on 25th December 2023]. Accessible at: <https://www.article19.org/resources/google-win-in-right-to-be-forgotten-case-is-victory-for-global-freedom-of-expression/>.

DE HERT, Paul. A right to identity to face the Internet of Things. Council of Europe Publishing [online]. 2007. [cit. on. 25th December, 2023]. Accessible at:

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

DIXIT, Priyanshi. Will The Internet Remember You Forever? Right To Be Forgotten And Its Territorial Limits [online]. IIPRD, 23th November, 2019 [cit. on. 25th December 2023]. Accessible at: <https://www.iiprd.com/will-the-internet-remember-you-forever-right-to-be-forgotten-and-its-territorial-limits/>

DRUMMOND, David. We Need to Talk about the Right to Be Forgotten. London: The Guardian [online]. 10th July 2014. [cit. on. 25th December 2023]. Accessible at: <https://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate>.

Facebook Help Centre: What is a legacy contact and what can they do? [online]. Accessible at: <https://www.facebook.com/help/1568013990080948>.

FALQUE-PERROTIN, Isabelle. Pour un droit au déréférencement Mondial. Debates du Monde. [online]. 12th January, 2017 [cit. on 25th December 2023]. Accessible at: <https://www.cnil.fr/fr/pourun-droit-au-dereferencement-mondial>.

FORDE, Aidan. Implications of the Right To Be Forgotten. Tulane Journal of Technology and Intellectual Property. 2015, Vol. 18., p. 107.

GSTREIN, Oskar J. The Judgment That Will Be Forgotten'. Verfassungsblog: On Matters Constitutional [online]. 25th September 2019. [cit. on. 25th December 2023]. Accessible at: <https://verfassungsblog.de/the-judgment-that-will-be-forgotten/>.

HOPKINS, Cathryn. Territorial scope in recent CJEU cases: Google v CNIL / Glawischnig-Piesczek v Facebook [online]. The International Forum for Responsible Media Blog, 9th November 2019 [cit. on. 16th December 2023]. Accessible at: <https://inforrm.org/2019/11/09/territorial-scope-in-recent-cjeu-cases-google-v-cnil-glawischnig-piesczek-v-facebook-cathryn-hopkins/>

HUSOVEC, Martin. Should We Centralize the Right to Be Forgotten Clearing House? Center for Internet and Society [online]. 30th May 2014, [cit. on. 25th December 2023]. Accessible at: <https://cyberlaw.stanford.edu/blog/2014/05/should-we-centralize-right-be-forgotten-clearing-house>.

IGLEZAKIS, Ioannis. The Right to be Forgotten: A New Digital Right for Cyberspace [online]. Segurança da informação e Direito Constitucional do ciberespaço, 26th December 2016 [cit. on 16th December 2023]// Accessible at:

<https://iglezakis.gr/2016/12/26/the-right-to-be-forgotten-a-new-digital-right-for-cyberspace/>;

Information Commissioner's Office. Data Protection Act of 1998 Supervisory Powers of the Information Commissioner Enforcement Notice [online], 2015. [cit. on 27th December 2023]. Accessable at: <https://ico.org.uk/media/action-weve-taken/mpns/2259545/ams-marketing-ltd-mpn-20180727.pdf>.

KETTEMANN, Matthias C.; Tiedeke, SOPHIA Anna. Welche Regeln, welches Recht? Glawischnig-Piesczek und die Gefahren nationaler Jurisdiktionskonflikte im Internet [online]. VerfBlog, 10th October 2019 [cit. on. 16th December 2023]. Accessible at: <https://verfassungsblog.de/welche-rechte-welches-recht/>;

LYNSKEY, Orla. Rising like a Phoenix: The «Right to be Forgotten» before the ECJ. THE EUROPEAN BLOG [online]. 13th May 2014. [cit on. 25th December 2023]. Accessible at: <http://europeanlawblog.eu/2014/05/13/rising-like-a-phoenix-the-right-to-be-forgotten-before-the-ecj/>

O'BRIEN, Danny, YORK, Jillian. Rights that Are Being Forgotten: Google, the ECJ, and Free Expression, Electronic Frontier Found [online]. 8th July 2014, [cit. on 23th December 2023]. Accessible at: <https://www.eff.org/deeplinks/2014/07/rights-are-being-forgotten-google-ecj-and-free-expression>.

OGHIA, Michael J. Information Not Found: The "Right to Be Forgotten" as an Emerging Threat to Media Freedom in the Digital Age. CIMA Digital Report [online]. 9th January 9 2018. [cit. on. 25th December 2023]. Accessible at: <https://www.cima.ned.org/publication/right-to-be-forgotten-threat-press-freedom-digital-age/>.

OkCupid's Terms and Conditions. [online]. Accessible at: <https://www.okcupid.com/legal/terms>.

PEERS, Steve. The CJEU's Google Spain Judgment: Failing to Balance Privacy and Freedom of Expression, EU Law Analysis. [online]. 13th May 2014 [cit. on. 25th December 2023], Accessible at: <http://eulawanalysis.blogspot.co.uk/2014/05/the-cjeus-google-spain-judgment-failing.html [http://perma.cc/T8QN-W2G2]>.

PIRKOVA, Eliška, MASSÉ Estelle. EU Court decides on two major "right to be forgotten" cases: there are no winners here. AccessNow [online]. 23th October 2019. [cit. on. 23th December 2023]. Accessible at: <https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/>.

Recital 23 GDPR. Also see: Article 29 Working Party, Opinion 8/2010 on Applicable Law, 2010, WP 179 28 [online]. Accessible at: <http://ec.europa.eu/justice/article-29/documentation>;

READING, Vivian. The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital, Life, Design Munich, 22 January 2012 <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26>.

READING, Viviane. The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age. SPEECH/12/26 [online]. 22th January 2012. [cit. On. 25th December 2023]. Accessible at:

REES, Marc. Droit à l'oubli: l'effet Streisand peut être évité dans les décisions de la CJUE. NextBeta [online]. 14th March 2017, [cit. on. 27th December 2023]. Accessible at: <https://www.nextinpact.com/article/25880/103671-droit-a-oubli-effet-streisand-peut-etre-evite-dans-decisions-cjue?fbclid=IwAR3KQQEmXTXq8ifKNeNl8y26xOAta-IfQHUrMkvzYfd5oJPrGD4ncBFzLLg>.

RICHTERICH, Rachel. L'intégrité numérique: le vrai combat pour nos données. LeTemps, [online]. 11 January 2019. [cit. on 25th December 2023]. Accessible at: <https://www.letemps.ch/profil/rachel-richterich?before=2019-01-29T11%3A28%3A00%2B01%3A00>.

RODOTÀ, Stefano. Dai Ricordi Ai Dati L' Oblio È Un Diritto?. La Reppublica.it [online]. 30th January 2012. [cit. on 25th December 2023]. Accessible at: <https://ricerca.repubblica.it/repubblica/archivio/repubblica/2012/01/30/dai-ricordi-ai-dati-oblio-un.html>.

ROSEN, Jeffrey. The Web Means the End of Forgetting [online]. 21 June 2010, [cit. on. 25th December 2023]. Accessible at: <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all>

SAMONTE, Mary. Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law [online]. European Law Blog, 29th October 2019 [cit. on 16th December 2023]// Accessible at: <https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/>.

SCHNEIER, Bruce. Why 'Anonymous' Data Sometimes Isn't. WIRED. [online]. 12th December 2007. [cit. on. 23th December 2023]. Accessible at: <https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/>.

SOLON, Olivia. EU 'Right To Be Forgotten' Ruling Paves Way for Censorship. WIRED [online]. 13th May 2014 [cit. on. 25th December, 2023]. Accessible at: <http://www.wired.co.uk/news/archive/2014-05/13/right-to-be-forgotten-blog>.

STUPARIU, Ioana. Defining the right to be forgotten: A Comparative Analysis between the EU and the US. Budapest: Central European University. LL.M. Short Thesis. 2015, 84 p.

VAN HOBOKEN, Joris V. J.. The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember. Freedom of Expression Safeguards in a Converging Information Environment. Prepared for the European Commission Appointment Letter No. 25797. [online]. 14th January 2013. [cit. on 25th December 2023].

WALKER, Kent. A Principle That Should Not Be Forgotten. Google Blog. [online]. 19th May 2016. [cit. on. 25th December 2023]. Accessible at: <https://blog.google/around-the-globe/google-europe/a-principle-that-should-not-be-forgotten/>.

Walter Sedlmayr. [online]. [cit. on. 25th December 2023]. Available at: <https://en.wikipedia.org/wiki/Walter_Sedlmayr>.

WOHLSEN, Marcus. For Google, the 'Right to Be Forgotten' Is an Unforgettable Fiasco. WIRED [online]. 3th July 2014. [cit. on. 25th December 2023]. Accessible at: <https://www.wired.com/2014/07/google-right-to-be-forgotten-censorship-is-an-unforgettable-fiasco/>.

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

Decisions of the Court of Justice of the European Union

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 16 December 2008. *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*. Case C-73/07.

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 September 2019. *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, para. 72.

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others*. 44 (2014)

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 October 2018, *Hessische Knappschaft v. Maison Singer and sons,* Case C-234/17.

Court of Justice of the European Union*: Judgment of the Court (Grand Chamber) of 13 May 2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González, Case C-131/12.

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 16 December 2008. *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*. Case C-73/07.

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. Case C-311/18.

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, Case C-210/16.

Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 20 December 2017, *Peter Nowak v. Data Protection Commissioner*. Case C-434/16.

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 8 December 2022. *TU and RE v Google LLC*. Case C-460/20.

Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 9 March 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, Case C-398/15

Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, Request for a preliminary ruling from the Supreme Court. Case C-434/16, para. 34.

Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 29 July 2019, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, Case C-40/17.

Court of Justice of the European Union: Judgment of the Court (Third Chamber) of 7 November 2013, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, C-473/12., para. 1–10.

Court of Justice of the European Union: Judgment of the Court (Third Chamber), 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, Case C-141/12.

Court of Justice of the European Union: Judgment of the Court of 24 September 2019. *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*. Case C-136/17.

Court of Justice of the European Union: Judgment of the Court of 11 December 2014. *František Ryneš v Úřad pro ochranu osobních údajů*. Case C-212/13.

Court of Justice of the European Union:Judgment of the Court (Grand Chamber) of 5 June 2018. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*. Case C-210/16. EU:C:2018:388.

Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14 EU:C:2016:779 and so on.

Court of Justice of the European Union: Judgment of the Court (Third Chamber) of 1 October 2015, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*. Request for a preliminary ruling Case C-230/14.

Court of Justice of the European Union: Judgment of the Court (Third Chamber) of 28 July 2016. *Verein für Konsumenteninformation v Amazon EU Sàrl.* Case C-191/15.

Court of Justice of the European Union: Judgment of the Court of 14 May 1974. *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*. Case 4-73.

Court of Justice of the European Union. Judgment of the Court of 20 May 2003. *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk*. Joined cases C-465/00, C-138/01 and C-139/01.

Court of Justice of the European Union: Judgment of the Court of 6 November 2003, *Criminal proceedings against Bodil Lindqvist*, Case C-101/01.EU:C:2003:596;

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 29 January 2008. *Productores de Música de España (Promusicae) v Telefónica de España SAU*. C-275/06. pp. 309-348.

Opinion of Advocate General Jääskinen delivered on 25 June 2013.

Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13th May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. Case C-131/12: ECLI:EU:C:2013:424.

Opinion of Advocate General Szpunar delivered on 4 June 2019.Eva Glawischnig-Piesczek v Facebook Ireland Limited. Case C-18/18: ECLI identifier: ECLI:EU:C:2019:458.

Opinion of Advocate General Trstenjak delivered on 18 May 2010. Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09). Joined cases C-585/08 and C-144/09:ECLI:EU:C:2010:273.

Decisions of the European Court on Human Rights

ECtHR: Judgment of the Court of 24 September 2007, *Tysiąc v Poland*. Application No. 5410/03.

ECtHR: Judgment of the Court of 16 July 2013, *Węgrzynowski and Smolczewski v. Poland.*Application No. 33846/07.

ECtHR, Fifth Section, Judgment of 19 October 2017. *Fuchsmann v. Germany.* Application no. 71233/13.

ECtHR, Fifth Section, Judgment of *M. L. and W. W. v. Germany*, Applications nos. 60,798/10 and 65,599/10, September 28, 2018.

ECtHR, Fourth Section, Judgment of July 16, 2013. *Węgrzynowski and Smolczewski v. Poland*, Application no. 33846/07.

ECtHR: Judgment of 10 December 1984, *Acmanne and Others v. Belgium*, Application no. 10435/83.

ECtHR: Judgment of 12 January 2010, *Gillan v. Quinton v the United Kingdom*, Application no. 4158/05

ECtHR: Judgment of 12 January 2016. *Genner v. Austria*, Application no. 55495/08.

ECtHR: Judgment of 13 December 1979, *X v. Austria*, Application no. 8278/78.

ECtHR: Judgment of 13 July 2006. *Jäggi v. Switzerland*, Application no. 58757/00.

ECtHR: Judgment of 14 October 2021, *M.L. v. Slovakia*, Application no. 34159/17.

ECtHR: Judgment of 15 May 2006. *The Estate Of Kresten Filtenborg Mortensen v. Denmark*, Application no. 1338/03.

ECtHR: Judgment of 16 June 2015, *Delfi AS v. Estonia*, Application. no. 64569/09.

ECtHR: Judgment of 17 December 2012, *Koch v Germany*, Application. no. 497/09, para 78.

ECtHR: Judgment of 18 October 2011, *Khelili v. Switzerland,* Application. no. 16188/07).

ECtHR: Judgment of 19 September 2017, *Tamiz v. the United Kingdom*, Application no. 3877/14.

ECtHR: Judgment of 20 June 2019, *A and B v. Croatia,* Application. no. 7144/15.

ECtHR: Judgment of 22 April 1997, *X, Y and Z v. The United Kingdom*, Application 75/1995/581/667.

ECtHR: Judgment of 25 February 2022, *Biancardi v. Italy*, Application. no. 77419/16.

ECtHR: Judgment of 28 June 2006, *Thevenon v. France*, Application. no. 2476/02.

ECtHR: Judgment of 7 February 2012, *Von Hannover v. Germany (№ 2)*, Applications. nos. 40660/08 and 60641/08;

ECtHR: Judgment of 7 February 2012, *Axel Springer AG v. Germany*, Application № 39954/08

ECtHR: Judgment of 9 December 2014, *Yakovlevich Dzhugashvili v. Russia*, Application no. 41123/10.

ECtHR: Judgment of Grand Chamber of 4th December 2008. *S. and Marper v. The United Kingdom*. Application Nos. 30562/04 and 30566/04.

ECtHR: Judgment of *Sanles Sanles v. Spain*, Application no. 48335/99, ECHR 2000-XI.

ECtHR: Judgment of the Court of 18th October 2011, *Khelili v Switzerland* .Application no. 16188/07.

ECtHR: Judgment of the Court of 28th June 2018, Case of *M.L. and W.W. v. Germany*. Applications nos. 60798/10 and 65599/10

ECtHR: Judgement of 8 July 1986, *Lingens v. Austria*, Application. no. 9815/82.

ECtHR: Judgment of the Court of 19 September 2017, *Tamiz v. United Kingdom.* Application no. 3877/14

ECtHR: Judgment of the Court of 4 September 2019, *Einarsson v. Iceland. Application no. 39757/15*

ECtHR: Judgment of the Court of 19 January 2018, Case of *Fuchsmann v. Germany.* Application no. 71233/13.

EU legal documents

Charter of Fundamental Rights of the European Union (2012/C 326/02) (CFR).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

OJ L 119, 4.5.2016, p. 1–88

Universal Declaration of Human Rights (10 Dec. 1948), U.N.G.A. Res. 217 A (III) (1948).

UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).

Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969.

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

UN Human Rights Committee (HRC), *General comment no. 34, Article 19, Freedoms of opinion and expression*, 12 September 2011, CCPR/C/GC/34.

Council of Europe: Committee of Ministers, Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, 4 April 2012.

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' (European Parliament, 12 March 2014) accessed 24 October 2019.

Consolidated version of the Treaty on the Functioning of the European Union Official Journal 115, 09/05/2008 P. 0164 – 0164.

United Nations General Assembly. The Universal Declaration of Human Rights (UDHR). New York: United Nations General Assembly, 1948.

International Covenant on Civil and Political Rights (adopted 19 December 1966, entered into force 23 March 1976) 999 UNTS 171, Article 17.

Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981).

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), 128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018)

The Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) OJ L 178, 17.7.2000, p. 1–16.

Article 29 Working Party, 'Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgment in Google Spain' (n 691), pp. 5–6

Directive 95/46/EC of the European Parliament and of the Council of 24 October on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ 1995 L 281/31; 1995: 31–50.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007)

Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf(2018)15-final, 128 Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018).

Other acts and legal resources

Italian personal data protection Code/ Legislative Decree no. 196 of 30 June 2003.

Legislative Decree n. 101/2018 of September 4, 2018.

the French Act No. 2018-493 of 20 June 2018, Ordinance No. 2018-1125 of 12 December 2018.

Spanish Organic Law No. 6/1985 of July 1, 1985, on the Judicial Power (as amended up to Organic Law No. 4/2018 of December 28, 2018).

Swedish Personal Data Protection Act (Sw. Personuppgiftslag (1998:2014)).

Bundesdatenschutzgesetz 1977.

Judgment of the Supreme Court of 11th December 1939, file No. 308 U.S. 338.

Judgment of the Supreme Court of California, Briscoe v. Reader's Digest Association, Inc., L.A. No. 29813 [4 Cal.3d 529, 93 Cal. Rptr. 866, 483 P.2d 34]. (Cal. 1971).

Supreme Court of California, Barbara Streisand v. Kenneth Adelman Et. Al., Case No. SC077257, County of Los Angeles.

Das Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949.

List of abbreviations

CFR – The EU Charter on Fundamental Rights;

CJEU – Court of Justice of the European Union;

CNIL – French Data Protection Authority (Commission nationale de l'informatiqueet des libertés);

Convention 108 – Convention on the Protection of Natural Persons with regard to the Automated Processing of Personal Data adopted in 1981;

DMA – Digital Markets Act;

DPA – Data Protection Authorities;

DPD – Directive 95/46/EC;

DSA – Digital Services Act;

ECD – E-Commerce Directive;

ECHR (Convention) – European Convention on Human Rights;

ECtHR –European Court of Human Rights;

EU – European Union;

FCoS – French Council of State (Conseil d'État);

GDPR – General Data Protection Regulation;

Google Spain – The Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Case C-131/12;

Google v. CNIL – Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 24 September 2019. *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL),* Case C-507/17;

Piesczek v. Facebook (Glawischnig-Piesczek) – Court of Justice of the European Union: Judgment of 3th October 2019. *Eva Glawischnig-Piesczek v Facebook Ireland Limited.* Case C-18/18;

RTBF – Right to be Forgotten;

TFEU – Treaty on the Functioning of the European Union

WP29 – Article 29 Working Party.

Summary and keywords (EN)

The title of dissertation (Ph.D.) thesis: The Development of the Right to be forgotten in EU law: Challenges and Perspectives

Author: Hovsep Kocharyan

Keywords: European Union, right to be forgotten, privacy, data protection, digital identity, EU law, territorial scope, personal data.

The processing of personal data on the Internet nowadays is an inevitable part of human life. As soon as personal data is disclosed (primarily in the field of the Internet), it is usually available for an indefinite period of time. However, such practices create new serious risks of violating the privacy and there is a need to develop new legal mechanisms for their prevention. The right to be forgotten, particularly in relation to digital space and internet activities, is a contemporary legal phenomenon that reaches high relevance within the contemporary legal research. Nowadays, more than ever, a comprehensive and detailed analysis of this right in the current legal reality of the EU is more than necessary. This need is due to the fact that the question of the correlation of the right to be forgotten (as the new "internet" human right) with such classical human rights as respect for private and family life, protection of personal data, freedom of expression and information is brought to the fore. On the one hand, article 11 CFR enshrines freedom of expression and information, but on the other hand, the case law of the CJEU recognizes the existence of the right to be forgotten. In addition, the case law of the CJEU on the territorial scope of the right to be forgotten on the one hand limits its scope to the territory of the EU, and on the other allows its global application. The questions naturally arise: How does the right to be forgotten relate to the above-mentioned fundamental human rights? Do the criteria for the application of the right to be forgotten set out in the EU legislation and the case law of the CJEU allow to minimize the risk of conflicts between these rights? Are there any conflicts or contradictions in the CJEU's conclusions regarding the application of the right to be forgotten, and if so, what are the ways to resolve them. The study of the phenomenon of the right to be forgotten also involves a comparative and in-depth analysis of the judicial approaches of both the CJEU and the ECtHR in order to determine its place in the human rights system, identify problematic aspects of application and interrelation, new development

prospects and propose reasoned ways to resolve possible contradictions that may reduce the effectiveness of the protection of the person in the digital sphere.

This thesis is a comprehensive analysis of current EU legislation and the case law of the CJEU. It clearly defines the essence and nature of the right to be forgotten, its justifications, rationale, problematic aspects of the relationship between the right to be forgotten and the right to respect for private and family life, freedom of expression and information, as well as the problems of territorial application of the right to be forgotten, the challenges, risks and contradictions in the development of the right to be forgotten are identified and appropriate recommendations are proposed to minimize them.

The research goal of my dissertation thesis is to identify the essence and nature of the right to be forgotten, its scope, justification, its place in the system of protection of human rights; identification of effective judicial protection of the right to be forgotten in the current EU legislation, and in the judicial practice of the CJEU; analysis of problematic aspects of its correlation between the right to be forgotten with the right to respect for private and family life, freedom of expression and information; analysis of problematic aspects of territorial scope of application taking to account the latest case law of the CJEU and ECtHR, investigate new challenges in development of the right and suggest ways for their solution.

In this thesis, I focused primarily on the following two basic research questions:

1. What is the right to be forgotten?
2. What are the problematic aspects of the correlation between the right to be forgotten and respect for private and family life and freedom of expression and information within the EU, and how they can be solved?
3. What are the risks of effective judicial protection of the right to be forgotten created by the contemporary case law of the CJEU and ECtHR, and how they can be solved?

This thesis consists of an introduction, five chapters and a conclusion. After a general introduction, which includes a statement of the objectives of the work, definition of research issues, hypotheses and a description of the content of the dissertation, it follows the chapter named *"Privacy in Digital society: concepts and new foundations"* which provides a brief course on the development of the right to privacy, classifies the features of the basic concepts of privacy, identifies the main risks to privacy and data protection in the context of the datification of society.

The Chapter *"Introducing the right to be forgotten"* attempts to reveal the essence of the right to be forgotten in the context of various concepts of its justification, disclosure of its legal

nature, as well as critically examines the main doctrinal definitions of the right in question, gives its own definition of the right in question. Defining the Google Spain case as a branchmark for the right to be forgotten, nevertheless, its achievements are critically evaluated and the conclusion is drawn that the right to be forgotten is much broader than indicated in the judicial practice of the EU, including in the "post-Gogglespain" period, and it does not boil down to the right to erasure or to the procedural rules specified in the GDPR.

The Chapter *"The scope of application of the right to be forgotten in practice"* examines the scope of the right to be forgotten, reveals the concept of personal data and its elements. It is concluded that the CJEU adheres to a broad interpretation of the elements of the definition of personal data, which makes it possible to extend the right to be forgotten to a broader area of personal data protection than indicated in EU case-law.

The Chapter *"Finding balance between the right to be forgotten and freedom of Expression"* is devoted to discussing the balance between the right to be forgotten and freedom of Expression. The judicial practice of the CJEU and the ECtHR is being considered to identify criteria for such balancing, and to discuss the issue of balancing in the doctrine. The critical analysis shows the discrepancy between the grounds, justification and scope of the right to be forgotten in the legal practice of the European Courts.

The Chapter *"The right to be forgotten: Challanges and perspectives for EU Data Protection Law"* is devoted to discussing the prospects for development and the challenges of further development of the right to be forgotten. I conclude that the scope of the right to be forgotten should be expanded and the right to personal identity and human dignity should be considered as a justification. This approach will make it possible to extend this right to the sphere of protection of post-mortem privacy as well and further increase the effectiveness of human protection in the digital sphere. The issues of territorial application of the right to be forgotten are considered, in particular in the context of the possibility of its global spread. Having reviewed the case law of CJEU, I come to the conclusion that the CJEU is faced not with a choice between local and global application of the right to be forgotten, but rather with the need to develop criteria that would help regulate the application of EU data protection legislation outside the EU borders.

In conclusion, the main conclusions drawn during the study are summarized and the necessary recommendations are given for the further development of the right to be forgotten.

The main hypotheses of this doctoral thesis are as follows:

1. The Right to be forgotten has a potential to serve as legal mechanism, allowing the deletion of personal data left on the Internet in order to protect the individual, his dignity, reputation, privacy and identity in the online world.
2. There are visible distinctions in understanding of the scope and content of the Right to be forgotten in the relevant case law of key European supranational courts.

Both hypotheses are tested in parallel via critical analyses of the case-law and its developments.

Shrnutí a klíčová slova (CZ)

The title of dissertation (Ph.D.) thesis: Vývoj práva být zapomenut v právu EU: výzvy a perspektivy

Autor: Hovsep Kocharyan

Klíčová slova: Evropská unie, právo být zapomenut, soukromí, ochrana údaje, digitální identita, právo Evropské unie, územní působnost, osobní údaje

Zpracování osobních údajů na internetu je v dnešní době nevyhnutelnou součástí lidského života. Jakmile jsou osobní údaje zveřejněny (především v oblasti Internetu), jsou obvykle k dispozici na dobu neurčitou. Takové praktiky však vytvářejí nová vážná rizika narušení soukromí a je třeba vyvinout nové právní mechanismy pro jejich prevenci. Právo být zapomenut, zejména ve vztahu k digitálnímu prostoru a internetovým aktivitám, je současným právním fenoménem, který dosahuje vysokého významu v rámci současného právního výzkumu. V dnešní době, více než kdy jindy, je komplexní a podrobná analýza tohoto práva v současné právní realitě EU více než nezbytná. Tato potřeba je dána skutečností, že se do popředí dostává otázka korelace práva být zapomenut (jako nového "internetového" lidského práva) s tak klasickými lidskými právy, jako je respektování soukromého a rodinného života, Ochrana osobních údajů, svoboda projevu a informací [viz články 7, 8 a 11 Listiny základních práv Evropské unie (2012/C 326/02). // URL: http://data.europa.eu/eli/treaty/char_2012/oj]. Na jedné straně Článek 11 CFR zakotvuje svobodu projevu a informací, ale na druhé straně judikatura SDEU uznává existenci práva být zapomenut. Kromě toho judikatura Soudního dvora EU o územní působnosti práva být zapomenut na jedné straně omezuje jeho působnost na území EU a na druhé straně umožňuje jeho globální aplikaci. Přirozeně vyvstávají otázky: jak souvisí právo být zapomenut s výše uvedenými základními lidskými právy? Umožňují kritéria pro uplatnění práva být zapomenut stanovená v právních předpisech EU a judikatuře Soudního dvora EU minimalizovat riziko konfliktů mezi těmito právy? Existují nějaké konflikty nebo rozpory v závěrech SDEU ohledně uplatňování práva být zapomenut, a pokud ano, jaké jsou způsoby jejich řešení. Studium fenoménu práva být zapomenut zahrnuje také srovnávací a hloubkovou analýzu soudních přístupů SDEU i ESLP s cílem určit jeho místo v systému lidských práv, identifikovat problematické aspekty aplikace a vzájemného vztahu,

nové vyhlídky na rozvoj a navrhnout odůvodněné způsoby řešení možných rozporů, které mohou snížit účinnost ochrany osoby v digitální sféře.

Tato práce je komplexní analýzou současné legislativy EU a judikatury Soudního dvora EU. Jasně definuje podstatu a povahu práva být zapomenut, jeho zdůvodnění, zdůvodnění, problematické aspekty vztahu mezi právem být zapomenut a právem na respektování soukromého a rodinného života, svobodu projevu a informací, jakož i problémy územní aplikace práva být zapomenut, jsou identifikovány výzvy, rizika a rozpory ve vývoji práva být zapomenut a jsou navržena vhodná doporučení k jejich minimalizaci.

Výzkumným cílem mé disertační práce je identifikovat podstatu a povahu práva být zapomenut, jeho rozsah, zdůvodnění, jeho místo v systému ochrany lidských práv; identifikace účinné soudní ochrany práva být zapomenut v současné legislativě EU a v soudní praxi Soudního dvora EU; analýza problematických aspektů jeho korelace mezi právem být zapomenut a právem na respektování soukromého a rodinného života, svobody projevu a informací.; analýza problematických aspektů územní působnosti s přihlédnutím k nejnovější judikatuře Soudního dvora EU a ESLP, zkoumání nových výzev ve vývoji práva a navrhování způsobů jejich řešení.

V této práci jsem se zaměřil především na následující dvě základní výzkumné otázky:

1. Jaké je právo být zapomenut?
2. Jaké jsou problematické aspekty vztahu mezi právem být zapomenut a respektem k soukromému a rodinnému životu a svobodou projevu a informací v rámci EU a jak je lze řešit?
3. Jaká jsou rizika účinné soudní ochrany práva být zapomenut vytvořená současnou judikaturou Soudního dvora EU a ESLP a jak je lze řešit?

Tato práce se skládá z úvodu, pěti kapitol a závěru. Po obecném úvodu, který obsahuje vyjádření cílů práce, vymezení výzkumných otázek, hypotéz a popis obsahu disertační práce, navazuje na kapitolu s názvem "*Soukromí v digitální společnosti: koncepty a nové základy*", která poskytuje stručný kurz o vývoji práva na soukromí, klasifikuje rysy základních pojmů soukromí, identifikuje hlavní rizika pro soukromí a ochranu dat v kontextu datifikace společnosti.

Kapitola *"Zavedení práva být zapomenut"* se pokouší odhalit podstatu práva být zapomenut v kontextu různých konceptů jeho ospravedlnění, zveřejnění jeho právní povahy a kriticky zkoumá hlavní doktrinální definice dotyčného práva, dává vlastní definici dotyčného práva. Definování případu Google Spain jako branchmark pro právo být zapomenut, nicméně

jeho úspěchy jsou kriticky hodnoceny a dochází k závěru, že právo být zapomenut je mnohem širší, než je uvedeno v soudní praxi EU, včetně období "post-Gogglespain", a neomezuje se na právo na výmaz nebo na procesní pravidla uvedená v GDPR.

Kapitola *"Rozsah uplatnění práva být zapomenut v praxi"* zkoumá rozsah práva být zapomenut, odhaluje pojem osobních údajů a jeho prvky. Dospělo se k závěru, že SDEU dodržuje široký výklad prvků definice osobních údajů, což umožňuje rozšířit právo být zapomenut na širší oblast ochrany osobních údajů, než je uvedeno v judikatuře EU.

Kapitola *"Nalezení rovnováhy mezi právem být zapomenut a svobodou projevu"* je věnována diskusi o rovnováze mezi právem být zapomenut a svobodou projevu. Soudní praxe Soudního dvora EU a EÚLP se zvažuje, aby určila kritéria pro takové vyvažování a diskutovala o otázce vyvažování v doktríně. Kritická analýza ukazuje rozpor mezi důvody, zdůvodněním a rozsahem práva být zapomenut v právní praxi evropských soudů.

Kapitola *"Právo být zapomenut: výzvy a perspektivy práva EU na ochranu údajů"* je věnována diskusi o perspektivách rozvoje a výzvách dalšího rozvoje práva být zapomenut. Dospěl jsem k závěru, že rozsah práva být zapomenut by měl být rozšířen a právo na osobní identitu a lidskou důstojnost by mělo být považováno za ospravedlnění. Tento přístup umožní rozšířit toto právo i na oblast ochrany posmrtného soukromí a dále zvýšit účinnost ochrany člověka v digitální sféře. Jsou zvažovány otázky územní aplikace práva být zapomenut, zejména v souvislosti s možností jeho globálního rozšíření. Po přezkoumání judikatury Soudního dvora Evropské unie jsem dospěl k závěru, že Soudní dvůr není postaven před volbu mezi místním a globálním uplatňováním práva být zapomenut, ale spíše před potřebu vypracovat kritéria, která by pomohla regulovat uplatňování právních předpisů EU o ochraně údajů mimo hranice EU.

Závěrem jsou shrnuty hlavní závěry vyvozené během studie a jsou uvedena nezbytná doporučení pro další rozvoj práva být zapomenut.

Hlavní hypotézy této disertační práce jsou následující:

1. Právo být zapomenut má potenciál sloužit jako právní mechanismus umožňující vymazání osobních údajů ponechaných na internetu za účelem ochrany jednotlivce, jeho důstojnosti, pověsti, soukromí a identity v online světě.
2. V příslušné judikatuře klíčových evropských nadnárodních soudů jsou viditelné rozdíly v chápání rozsahu a obsahu práva být zapomenut.

Obě hypotézy jsou paralelně testovány prostřednictvím kritických analýz judikatury a jejího vývoje.