DOI 10.5817/MUJLT2023-1-3

THE UNWANTED PARADOXES OF THE RIGHT TO BE FORGOTTEN *

by

LUSINE VARDANYAN † HOVSEP KOCHARYAN ‡
ONDREJ HAMUĽÁK § MATÚŠ MESARČÍK ¶
TANEL KERIKMÄE || TEA KOOKMAA **

The dynamic development of digital and informational technologies raises the issue of proper and effective protection of human privacy, which, in turn, is gradually turning from a real fundamental right into a kind of illusion. Just a piece of information about an individual distributed on the Internet may leave its negative and often indelible mark on the life and reputation of the addressee of such information, regardless of the legality and reliability of such information. And even if such information is subsequently recognized as false and/or vicious and even removed from public access, the addressee of the information will still be associated with such information in the social consciousness. In this regard, each person is at risk on the Internet, where anyone can potentially become the victim of a single publication or a post of an Internet user. In this context the emergence of the phenomenon of the right to be forgotten in European legal reality may be considered as a step forward in the question of human privacy protection in the digital age. However, this right is not without drawbacks. The most significant of these drawbacks will be analyzed in this paper, such as the practical difficulties

* The paper has been prepared on behalf of the project GAČR no. 20-27227S "The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union" funded by the Czech Science Foundation.

† Lusine Vardanyan, lusine.vardanyan01@upol.cz, Ph.D. Candidate, Palacký University Olomouc, Faculty of Law, Czech Republic;

‡ Hovsep Kocharyan, hovsep.kocharyan01@upol.cz, Ph.D. Candidate, Palacký University Olomouc, Faculty of Law, Czech Republic

§ Ondrej Hamuľák (corresponding author), ondrej.hamulak@upol.cz, Senior Researcher, Palacký University Olomouc, Faculty of Law, Czech Republic

¶ Matúš Mesarčík, matus.mesarcik@flaw.uniba.sk, Assistant Professor, Comenius University in Bratislava, Faculty of Law, Slovakia

|| Tanel Kerikmäe, tanel.kerikmae@taltech.ee, Professor of European Legal Policy and Law Tech, Tallinn University of Technology (TalTech), Department of Law, Estonia

** Tea Kookmaa, tea.kookmaa@njordlaw.ee, Attorney-at-law, NJORD Law Firm, Estonia

of thoroughly exercising this right and the difficulties posed by new technological developments.

KEY WORDS
right to be forgotten, privacy, GDPR, technology, innovation

1. INTRODUCTION
The right to be forgotten (the right to erasure) is a deeply interconnected with the judicial law-making activity of the CJEU. Its significant development in the European legal reality is connected with an unprecedented case of Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) (known as the Google Spain case or Costeja case), where the Court ruled that: "the data subject may (...) require those links (concerning him/her) to be removed from the list of (search) results", "(...) in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed"[1]. The CJEU's judgment naturally caused a number of questions and discussions regarding the essence and nature of this right. In particular, some experts have critically perceived the emergence of the phenomenon of the right to be forgotten, consideringit as "unforgettable fiasco, (...) morphing into a nightmare for the web giant"[2], "an emerging threat to media freedom in the digital age"[3], "that threatens to censor entire swathes of the web"[4]. However, despite the existence of critical views, other scholars, on the contrary, reacted positively to the Court's judgment, arguing that the right to be forgotten as a privacy-protective right, that can exist side-by-side with freedom of expression and information, and with a reasonable delineation of their borders and an effective balancing of their coexistence, such a right can provide the data subject with opportunity to perform his/her privacy protection on the "eternal" Internet. As L. Cook points out: "The right

[1] Judgement of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317 (herein after "Google Spain"), paragraph 98, paragraph 94.

[2] Wohlsen, M. (2014) For Google, the 'Right to Be Forgotten' Is an Unforgettable Fiasco. *WIRED* Available from: https://www.wired.com/2014/07/google-right-to-be-forgotten-censorship-is-an-unforgettable-fiasco/

[3] Oghia, M. J. (2018) Information Not Found: The "Right to Be Forgotten" as an Emerging Threat to Media Freedom in the Digital Age. *CIMA Digital Report*. Available from: https://www.cima.ned.org/publication/right-to-be-forgotten-threat-press-freedom-digital-age/

[4] See Solon, O. (2014) EU 'Right To Be Forgotten' Ruling Paves Way for Censorship. *WIRED* Available from: http://www.wired.co.uk/news/archive/2014-05/13/right-to-be-forgotten-blog

to be forgotten represents a positive shift in cyberspace law and policy because it increases individuals' control over personal information, and restores the balance between free speech and privacy in the digital world"[5], in the conditions when "(...) the Internet has robbed individuals of both privacy and autonomy in a sense that we no longer have the choice to keep certain information private, nor do we have the freedom not to speak"[6].

As we can see, before the right to be forgotten was written into the law, it had already been extended via interpretation of the right to erasure as one of the rights of the data subject by the CJEU in its case-law. In the year 2016, the European Commission adopted a new regulation – the Regulation (EU) 2016/679 of the European Parliament and of the Council, also known as the General Data Protection Regulation (the GDPR). The aim of adopting a new regulation was to create unified data protection related rules in all Member States of the EU. In several aspects, the GDPR resembles its predecessor, Directive 95/46/EC of the European Parliament and of the Council. Most of the general principles related to data protection, as well as the obligations applicable to data processing entities are similar to those in the Directive. However, the GDPR also stipulates new obligations for data processing entities. In addition, the GDPR specifies certain data subjects' rights and stipulates a few new ones. In its Article 17, the GDPR stipulates that the data subject "shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies." The grounds for exercising the right to be forgotten are specified in Article 17(1).

However, the implementation of the right to be forgotten in legal practice is not without drawbacks, naturally leaving its negative mark on the effectiveness of protecting the data subjects' privacy in the digital age, which will be analysed in more detail below. Although several statistics exist concerning the effectiveness of the right to be forgotten[7], the authors aim to point out paradoxes provided by the exercise of the right in question that may significantly influence the outcome in a negative way and ultimately diminish the protection of an individual.

The goal of the article is to discuss the challenges for the right to be forgotten from three angles – the jurisprudence of the CJEU,

---

[5] Cook L. (2015) The Right to Be Forgotten: A Step in the Right Direction for Cyberspace Law and Policy. Journal of Law, Technology & Internet 6(1). Available from: https://scholarlycommons.law.case.edu/jolti/vol6/iss1/8

[6] Ibid.

[7] See e.g. Google Transparency Report on delisting requests.Available from: https://transparencyreport.google.com/eu-privacy/overview.

regulatory provisions and emerging new concepts in technology. In the first part of the article, the authors will provide an overview of drawbacks of the right to be forgotten considering the selected paradoxes deriving from the jurisprudence of the CJEU and regulatory provisions. In sections two and three of the article authors analyse two landmark decisions of the CJEU that create unwanted paradoxes of remembering claimants despite their efforts to be forgotten. However, shortcomings of the right to be forgotten are not inherited only through the decisions of the CJEU. The fourth part of the article discusses regulatory gaps concerning the reflection of the right in the GDPR. The fifth section provides an analysis of potential challenges raised by new technologies and related new concepts as the emergence of this virtual space represents an ideal laboratory for further discussion on remembering and forgetting in the digital world. Conclusions are provided at the end of the article.

2. COSTEJA'S UNFORGETTABLE PARADOX: HOW TO BE UNINTENTIONALLY REMEMBERED?

The growing interest in the right to be forgotten is due to the fact that nowadays ensuring the protection of the right to privacy as one of the fundamental human rights in the EU is one of the most important tasks of the EU human rights law, which still remains as a real headache for the EU lawmakers, especially in the conditions of rapid development of digital technologies. In this framework, the CJEU's ruling may be considered as a sort of response to intervention in human privacy and a step forward for finding an effective *status quo* between the right to privacy and freedom of expression and information[8], because "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"[9].

However, being the cradle of the right to be forgotten, the CJEU nonetheless makes serious mistake in its judgments, which naturally leaves

[8] Concerning the human rights aspect of the decision, see paras 66 and 69 of the Google Spain case. The case itself is deliberated under the prism of Article 7 and Article 8 of the Charter of the fundamental rights of the European Union.

[9] Alessi, S. (2017) Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review* 32(1). Available from: `https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1186&context=eilr`

its negative mark on the effectiveness of protecting of the data subjects' privacy in the digital age. In this context naturally arise the questions on how the CJEU's judgment weakens the privacy-protective potential of this right? The answer is hidden in the description of the factual circumstances by the CJEU in its judgment on Google Spain case. In particular, the paragraph 14 of the case states that: "(...) 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."[10] As it can be noticed, from the very wording of the factual circumstances of the Google Spain case, it is possible to clearly understand what personal data the applicant wanted to hide from public access to protect his privacy. This is due to the fact that the Court not only described the applicant's name, neglecting the rules for maintaining the confidentiality of data subjects taking into account the essence and nature of the case under consideration, but also did not hide from public access the personal information that the applicant sought to remove from the Internet search engine.

In such circumstances, the following questions naturally arise: first, could it be considered that the CJEU's judgment effectively protected the privacy of Mr. Costeja González, and, second, is it possible in such conditions to call the Google Spain case as victorious for the applicant, and consider it as a victory in fact? We can safely answer no, since the Court only de jure protected the privacy of Mr. Costeja González, but de facto only inadvertently aggravated his situation. As we can see, even if the applicant, who applied to the court regarding the realization of his right to be forgotten, wins the court proceeding and achieves the removal of his undesirable personal data from the Internet, such personal data will still be publicly available (for example, on the CJEU's official websites: http://curia.europa.eu or https://eur-lex.europa.eu), where any Internet user can read, as, for example, the authors of this scientific research. And this is all just a 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. It turns out that the CJEU's judgment on the Google Spain case had the opposite effect on the data subject: it can be said that instead of the right to be forgotten, his right

[10] Google Spain case, para 14.

to be remembered was realized. Paradoxically, the CJEU itself became an 'undesirable PR manager' of the applicant, whose name is associated with the information on his insolvency and firmly entrenched in the public consciousness due to the works of various experts, scientists and journalists, turning his case into "a perfect example of the Streisand Effect in action"[11]. This fact is also emphasized by M. Xue, G. Magno and others, who tend to believe that: "Costeja himself suffers from the Streisand effect – although he won this landmark case, it is unlikely he will ever be forgotten because his name now appears on thousands of web sites".[12] The same opinion is held by A. Bunn, arguing that: "For Mr. González the decision has resulted in something of a curious irony: his bid not to be indefinitely linked through Google search to information concerning his debts was successful, but as a result of that success he is likely to be linked to the information he wished forgotten for a long time to come".[13] In his turn, P. W. Erikson points out that: "In a case of ultimate irony, Costeja González, who has been the subject of news stories around the world, will be now very difficult to ever forget. Perhaps his new celebrity status will offset any negatives".[14] In this context the Court's attitude to the presentation of the factual circumstances even allows to call the Google Spain case useless for the applicant, who, instead of getting rid of painful data, found himself in the public spotlight. According to G. Giampa: "(...) the sheer lack of respect for privacy along with the immediate gratification an individual receives through a Google search or Twitter feed. Costeja Gonzalez has inadvertently fought 'for the right[s] of others to more easily safeguard their privacy', but the principle outweighs the effects of the legal action"[15].

Of course, one can argue that this case was unprecedented for the Court's judicial practice, and the CJEU could not then foresee the effect of its judgment, which lead to the situation that "Mr. Costeja is better

---

[11] Holland, J.A. (2019) Contemporary Practical Alternatives to a "Right To Be Forgotten" in the United States. *Latin American Law Review* 2. Available from: https://revistas.uniandes.edu.co/doi/full/10.29263/lar02.2019.02

[12] Xue M., Magno G. et al. (2016) The Right to be Forgotten in the Media: A Data-Driven Study. *Proceedings on Privacy Enhancing Technologies 2016* (4). p. 1–14. Available from: http://www.nyu.engineering/sites/default/files/migrated/pdfs/RTBF_Data_Study.pdf

[13] Bunn, A. (2015) The curious case of the right to be forgotten. *Computer Law & Security Review* 31(3). p. 336 - 350. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0267364915000606

[14] Erikson, P.W. (2014) The EU's right to be forgotten. Available from: https://www.linkedin.com/pulse/20140710033506-2822374-the-eu-s-right-to-be-forgotten/

[15] Giampa, G. (2016) Americans Have a Right to Be Forgotten. *Law School Student Scholarship* 740. Available from: https://scholarship.shu.edu/student_scholarship/740/

known than before".[16] Although the mere fact of the unprecedented nature of the case cannot be considered as a justification for the Court's approach. Being the EU's highest judicial authority, it should understand the importance of careful description of the factual circumstances in its judgments to duly protect legitimate interests of the participants in the judicial process, especially in the conditions of the digital age, where the fragile privacy and reputation of a person very often become targets of the Internet community. As an example, we can take the case of the famous actress Barbra Streisand, who demanded the removal of the photo of her Malibu house taken by photographer Kenneth Adelman from the Internet, and her lawsuit only dramatically increased the number of views of this photo on the Internet, hence the name "Streisand effect", i.e. the effect of even greater spread of information when trying to hide or remove it from the public access.[17] Another example is the case of Max Mosley, who filed a lawsuit to protect his privacy and remove from the Internet his photos, containing sexual content, and although he won the case, the search results increased the frequency of references to the episode.[18]

It should be noted that such cases are numerous in practice, especially in the world of celebrities. The public is always interested in such 'forbidden' information, starting with unsuccessful photos of the American singer Beyonce[19] and ending with the romance of the Welsh footballer Ryan Giggs[20], because as it is said the forbidden fruit is always the sweetest. As A. De Baets rightly observes: "(...) any removal of documents would arouse curiosity and direct attention towards, rather than away from (...). Although the availability of digital information quickly publishable on the internet enhances both the disclosure of embarrassing information and tighter informational self-determination strategies, (...) the application of the right to be forgotten would not substantially affect the totality

[16] Schechner, S. (2014) Google Defends 'Right to Be Forgotten' Response. *Wall Street Journal*. Available from: https://www.wsj.com/articles/google-defends-right-to-be-forgotten-response-1416414403

[17] See Barbara Streisand vs. Kenneth Adelman et. al. Superior Court of California, County of Los Angeles, Case No. SC077257

[18] See Mosley v. News Group Newspapers [2008] EWHC 1777 (QB).

[19] See Zhang, M. (2013) Beyonce Publicist's Takedown Request Causes Unflattering Photos to Go Viral. *PetaPixel*. Available from: https://petapixel.com/2013/02/08/beyonce-publicists-takedown-request-causes-unflattering-photos-to-go-viral/

[20] See Masnick, M. (2011) Forget The Streisand Effect, I Think We've Seen The Dawning Of The Giggs Effect. *techdirt*. Available from: https://www.techdirt.com/articles/20110520/16102414365/forget-streisand-effect-i-think-weve-seen-dawning-giggs-effect.shtml

of sources for historians studying absolute public figures."[21] In such situations, the CJEU should not forget that in the digital world the issue of protecting the person's privacy and reputation becomes even more serious and vulnerable than protecting privacy and reputation offline. This means that it is necessary to be extremely careful in presenting the factual circumstances of the case and, if necessary, hide from public access information that can violate the applicant's privacy and reputation. And it cannot be said that the Court does not have such powers: it is enough to pay attention to the provision of Article 31 of the Protocol (No. 3) on the Statute of the Court of Justice of the European Union, providing that: "The hearing in court shall be public, unless the Court of Justice, of its own motion or on application by the parties, decides otherwise for serious reasons."[22] At the same time, the protection of the privacy, reputation and legitimate interests of the applicant can be safely considered as 'serious reasons' for the purposes of the above provision, because it is not by chance that the EU Charter on Fundamental Rights recognizes the fundamental nature of the rights to privacy and data protection[23].

3. PIESCZEK'S EFFECT AS A NEW EXAMPLE OF COSTEJA'S UNFORGETTABLE PARADOX?

It should be noted that the Costeja case is not the only case of the CJEU's 'blunder'. In the case of Eva Glawischnig-Piesczek v Facebook Ireland Limited, another victim of the Court's short-sighted approach in ensuring the applicant's privacy became the Austrian politician Eva Glawischnig-Piesczek, who appealed to the court for protection of her rights in connection with rude and offensive expressions of an Internet user about her. Analysing this case, it is possible to notice that the CJEU as in the case of Google Spain again forgets about the importance of ensuring the confidentiality of both the applicant herself and the information that caused the consideration of the case. Thus, in the Court's judgment the following factual circumstances are mentioned: "On 3 April 2016, a Facebook Service user shared on that user's personal page an article from the Austrian online news magazine

[21] De Baets, A. (2016) A historian's view on the right to be forgotten. *International Review of Law, Computers & Technology* 30(1-2). Available from: https://www.tandfonline.com/doi/full/10.1080/13600869.2015.1125155

[22] *Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 3) on the Statute of the Court of Justice of the European Union*, 7 June 2016 (C 202/210). Available from: http://data.europa.eu/eli/treaty/tfeu_2016/pro_3/oj

[23] See art. 7 and 8 of the *Charter of Fundamental Rights of the European Union* (2012/C, 326/02). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A12012P\%2FTXT

oe24.at entitled 'Greens: Minimum income for refugees should stay', which had the effect of generating on that page a 'thumbnail' of the original site, containing the title and a brief summary of the article, and a photograph of Ms Glawischnig-Piesczek. That user also published, in connection with that article, a comment which the referring court found to be harmful to the reputation of the applicant in the main proceedings, and which insulted and defamed her. This post could be accessed by any Facebook user."[24] Of course, unlike the Costeja case, the information, which is "harmful to the reputation of the applicant (…) which insulted and defamed her"[25], is not directly disclosed in the judgment, although it is still mentioned about the fact of insulting and slander against the well-known Austrian politician Ms. Glawischnig-Piesczek. However, it is impossible to blame only the Court: the Advocate General (AG), who made his opinion on this case may also be considered as a culprit. It is only necessary to pay attention to the paragraphs 12 and 14 of the Opinion of AG Szpunar, where applicant's data, as well as the subject of the case under consideration, are not kept confidential: "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'.[26] That is, if the fault of the Court was that it did not hide the applicant's identity in its judgment, then the AG is responsible for not initially hiding information, containing defamation against the Austrian politician, which, in turn, may be called as another example of manifestation of the 'Streisand effect' in the CJEU's judicial practice, because as D. Keller correctly notes: "On the claimant's side, the question is whether a filter effectively protects legitimate interests and rights — like the reputation and dignity rights at issue in Glawischnig-Piesczek. A clumsy filter, with conspicuous errors causing a 'Streisand effect' and additional negative attention to the claimant, might ultimately fail to protect her interests."[27] In his turn, M. Smith highlights that: "Facebook can be ordered to scrub those words—and any 'equivalent'

[24] Judgement of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, EU:C:2019:821, paragraph 12.

[25] Ibid.

[26] Opinion of AG Szpunar in Judgement of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, EU:C:2019:821, Recitals 12, 14.

[27] Keller, D. (2019) The CJEU's new filtering case, the terrorist content regulation, and the future of filtering mandates in the EU. *The Center for Internet and Society.* Available from: http://cyberlaw.stanford.edu/blog/2019/12/cjeu\%E2\%80\%99s-new-filtering-case-terrorist-content-regulation-and-future-filtering-mandates-eu

language—from its platform (...) worldwide. So says the European Court of Justice (ECJ). But if you perform a Google search for 'lousy traitor' and 'corrupt oaf' (even without the 'fascist party' label), your top hit will be a New York Times opinion piece identifying by name and photo (...) (of Eva Glawischnig-Piesczek)".[28]

As one can see, the case of Eva Glawischnig-Piesczek v Facebook Ireland Limited once again confirms the fact that such practice essentially weakens the effectiveness of the right to be forgotten, and this is one of the reasons why these right turn into just an illusive tool for the data subject in the context of his/her privacy protection in the court. As M. Cunningham correctly notes: "Europeans sought suppression of all these stories, which ironically boosted them further into the spotlight, creating a 'Streisand effect,' an attempt to hide information that spurs the unintended consequence of publicizing it more widely (...) and scores of others publish stories about the right to be forgotten generally and often cite to particular stories targeted for erasure".[29] Of course, this state of affairs may cause a negative impact on the CJEU's reputation and the EU citizens may have sceptical and even nihilistic views on the effectiveness of the Court's activities in the field of protecting their fundamental rights, and therefore the Court should change its approach when considering cases of this nature in order to avoid future manifestation of 'Costeja paradox' or 'Piesczek effect'. The Court should clearly understand that nowadays the contours of the formation of the right to be forgotten mostly depend on itself and it is not by chance that S. Kulk and F. Zuiderveen Borgesius note that: "The Court of Justice of the European Union gave limited guidance as to when a search result should be delisted (...) We can expect much more case law on delisting requests. More case law will hopefully lead to more guidelines for deciding delisting requests".[30] In the conditions of such an ineffective approach of the Court, the scenario of increasing case law on right to be forgotten cannot be expected, and thus this right may remain just a failed project, but not a real right that is able to protect human privacy and reputation. And if someone in such circumstances applies

[28] Smith, M. (2019) ANALYSIS: Global Censorship, but Not Erasure, Spurs Streisand Effect. *Bloomberg Law*. Available from: https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-global-censorship-but-not-erasure-spurs-streisand-effect.

[29] Cunningham, M. (2017) Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten. *Buffalo Law Review* 65(3). Available from: https://digitalcommons.law.buffalo.edu/cgi/viewcontent.cgi?article=4656&context=buffalolawreview

[30] Kulk S. and Borgesius, Z. F. (2017) Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe. In: Polonetsky, J., Tene, O. and Selinger E. (eds.) *Cambridge Handbook of Consumer Privacy*. Cambridge: Cambridge University Press. Available from: https://dare.uva.nl/search?identifier=f7d0f415-3404-426a-8833-12861fee7112

to the Court, most likely, the applicant's desire will not be the realization of his/her right to be forgotten, but on the contrary – his/her public exposition.

Another significant example regarding this issue is the ECtHR case of Hurbain v. Belgium.[31] Under the circumstances of this case, in 1994 in print edition of the Belgian daily newspaper Le Soir published an article about a fatal traffic accident caused by a drunk driver, as a result of which two people died and others were injured. The accident culprit stood trial and in 2006 he was rehabilitated. In 2011, he filed a lawsuit against Le Soir newspaper's publisher Patrick Hurbain, as a search on the applicant's last name immediately resulted in a link to the electronic archive of the newspaper Le Soir, where there was an article about the accident, which, according to the applicant, spoiled his reputation of a doctor, that is why he demanded to remove the text or at least hide his personal data from the article. As we can see, in this case, the same as in M.L. and W.W. v. Germany[32] and GC and Others v. CNIL[33] , only the name of the accident's culprit is concealed, but the factual circumstances capable of adequately protecting the anonymity of such a person are not concealed in any way. It should not be forgotten that the case concerned the removal of information from the electronic version of Le Soir's article, but not its print edition, and by detailing the circumstances of the accident, the Court still leaves open the possibility of identifying such a person, who, in turn, could become another victim of the 'Streisand effect'.

4. PRACTICAL DIFFICULTIES WHEN EXERCISING THE RIGHT TO BE FORGOTTEN

In addition to the jurisprudence of the CJEU discussed above, GDPR tries to take a step forward in ensuring that the data subject can effectively become forgotten. Article 17(2) stipulates the following: "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data". Article 17(2) is of significant importance in ensuring the effectiveness of the right to be forgotten in our digital age. Pursuant to Article 17(2),

[31] *Hurbain v. Belgium.* (2021) ECtHR, No. 57292/16.
[32] *W.W. v. Germany.* (2018) ECtHR, No. 60798/10 and 65599/10.
[33] Judgement of 24 September 2019, GC and Others v. CINIL, C-136/17, EU:C:2019:773.

we can understand that the controller has two obligations. First, when receiving a valid request for the right to be forgotten, erase all personal data itself. In addition, when the controller has made this personal data public, the controller must take reasonable steps to inform other controllers of this request as well. The aim of Article 17(2) is to ensure that even if the initial controller has shared the personal data to third parties (other controllers), then the personal data at their disposal will be deleted as well.

The obligation stipulated in Article 17(2) definitely contributes to effective execution of the right to be forgotten in the digital age. It can be said with certainty that in most cases, at least when personal data is being processed as part of digital services, the data controller at some point discloses the data subject's personal data to other controllers as well. For example, when the data controller shares the personal data of its client, for marketing purposes, with another company belonging to the same group of companies as the controller itself.

While the obligation stipulated in Article 17(2) constitutes as a positive step towards ensuring the effective implementation of the right to be forgotten, the obligation to notify other controllers also raises several practical issues. The wording of Article 17(2) stipulates that the controller must take reasonable steps to inform other controllers. In addition, two other conditions apply: the controller must take into account available technology and the cost of implementation. It is important to note that the obligation to notify other controllers can, in many circumstances, be difficult for the controller. The controller may not be able to track down all the other controllers to whom it has shared personal data. In addition, even if the controller is able to track down the other controllers to whom it has shared the personal data, it is important to note that these controllers may have disclosed the same personal data to other controllers again. Article 17(2) stipulates that the controller must take reasonable steps to inform other controllers about the data subject's request to erase the personal data. The GDPR does not give any guidance as to what constitutes a reasonable step to inform other controllers. It is understandable that a strict obligation to inform all the other controllers would be too impractical. Considering how often data controllers share personal data with their co-operation partners, clients or entities in other roles, it is understandable that we cannot expect a controller to be able to inform all the other controllers. In that sense, the wording take reasonable steps seems a good balance. This means that the controller must make sufficient effort to notify the other controllers or the right to be forgotten. However, the controller is not obliged to make an unreasonable effort. What shall be sufficient to qualify as reasonable

steps shall depend on who is the controller and what is the context of the personal data processing overall. In addition, the controller must take into account available technology and the cost of implementation. In practice, the latter means that if the controller needs to implement new technological solutions to carry out the informing, then in that case the controller should assess the cost of implementation. It can be understood from the wording of Article 17(2) that the controller that is the technological solution for performing the notification obligation is too expensive for the controller, then this may, depending on the context, constitute as a legitimate ground for not going forward with informing the other controllers. However, the authors of the article have seen in their professional legal practice that many controllers struggle with understanding what the notion of reasonable steps mean in a particular situation where they are considering whether to take additional actions to notify other controllers or not. In many cases, informing other controllers about the right to be forgotten request can be time-consuming as well as expensive. Since the term reasonable steps has not been clarified further in the GDPR, it remains very abstract for the controller and is subject to interpretation. It is very likely that due to a lack of specific guidelines for interpreting reasonable steps, many controllers would interpret this in favor of themselves. Also, based on the authors' experience as legal professionals, it is likely that many controllers would rather avoid making efforts to inform other controllers about the data subject's request. This means that it is questionable how effectively Article 17(2) contributes to the effective implementation of the right to be forgotten on the top of unwanted paradoxes discussed in previous sections.

5. TECHNOLOGICAL ADVANCEMENTS AS A NEW BATTLEFIELD

In the future, new technological developments can pose even greater risks for the right to be forgotten. In recent years, new technological concepts such as the metaverse, NFTs[34] and blockchain technology[35] have been widely talked about and the use of these technologies is getting closer and closer to the services and products which people engage in daily.

One of the most intriguing topics in the field of technology at the moment is the emergence of metaverse. As a concept, the metaverse means an independent world of virtual reality. In 2020, Facebook announced the new name of its brand – Meta.[36] The change in the name of the brand

[34] Non-fungible token.

[35] An advanced database mechanism that allows transparent information sharing within a business network.

[36] Meta. (2021) *Introducing Meta: A Social Technology Company.* [press release] 28 October.

reflects the social media giant's future plans to develop Facebook from a social media company to a metaverse company. Facebook's aim is to use the metaverse to help people connect better. Facebook's vision of metaverse is a mixture of both virtual and augmented reality which enables people – with the use of VR headsets and other tools – to connect with each other in a more efficient and real-life simulating way. In addition, metaverse would allow people to engage in various types of immersive experiences.

It is important to note that the metaverse is a very new concept. Although it is discussed widely among both technology and legal experts, the actual meaning of the concept still remains vague.[37] Different legal experts, scholars, as well as experts in the field of technology have defined metaverse in their own ways. For example, some authors have said that "the idea of a metaverse involves a computer-generated universe; a fully immersive online world where people gather to play games, socialize and work."[38] In contrast, other authors have described the metaverse as "a shared virtual world that users can access from any platform via the internet, and where they can interact with their virtual avatars."[39] The fact that metaverse is still a vague concept is partly also due to the fact that some technological advancements are still needed to launch the metaverse. The idea of the metaverse rather reflects the coming of a new era.

However, if the metaverse would turn out at least to a large extent in the way as it has been described, it would bring along various opportunities in almost all fields – social media, entertainment, e-commerce, education and many others.[40] For example, metaverse would allow customers of e-shops to try on clothes in the virtual world. Similarly, elementary school students could learn about forest trees by immersing themselves into a forest in the metaverse.

Available from: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

[37] It is important to note that different opinion leaders in technology have different views on what the "metaverse" would actually look like in reality. For example, see Hoffman, CH. (2021) What Is the Metaverse? Is It Just Virtual Reality, or Something More? *How-to Geek*. Available from: https://www.howtogeek.com/745807/what-is-the-metaverse-is-it-just-virtual-reality-or-something-more/

[38] (2022) *The British Journal of Criminology*, 62(6), 2022, Vol. 62, No. 6.

[39] EU. (2022) Legal issues in the metaverse / Part 1 - Introduction to the metaverse. *CMS Legal*. Available from: https://cms-lawnow.com/en/ealerts/2022/07/legal-issues-in-the-metaverse-part-1-introduction-to-the-metaverse\#:\~:text=What\%20is\%20the\%20metaverse\%3F,both\%2C\%20e.g.\%20through\%20VR\%20glasses.

[40] For example, see Balis, J. (2022) How Brands Can Enter the Metaverse. *Harvard Business Review*. Available from: https://hbr.org/2022/01/how-brands-can-enter-the-metaverse

While the metaverse would bring along unseen opportunities, several privacy experts have already expressed serious concerns about the privacy rights in the metaverse.[41] One author has pointed out: "We can expect companies in metaverse to collect personal information for individual identification, advertisement, and tracking through multiple channels, like wearable devices, microphones, heart and respiratory monitors, and user interactions to the extent that we have never seen before."[42] It is easy to understand that in the metaverse, the extent of personal data processing would be even greater than it is on the social media platform which we are using today. Therefore, data protection and data subject's rights in the metaverse would be more difficult to achieve. The question of how to protect data subjects' rights in the metaverse needs great attention.

As we have discussed previously, the metaverse can mean that there will be a need for new and fundamentally different privacy related legal acts. What about the right to be forgotten? Will it be difficult or even impossible to enforce the right to be forgotten in the metaverse? Here, there are different opinions. First, most privacy experts agree that it could be much more difficult to enforce the right to be forgotten due to the even more rapid pace of sharing personal data between different data processors. This means that upon receiving a request to have personal data erased, it can prove impossible for the controller to delete the data, as it is already being processed by so many other service providers in the metaverse despite the obligation in the Article 17 (2) GDPR as discussed above. It is also important to remember that it could be difficult for supervisory authorities to carry out supervisory proceedings in the metaverse. It can be difficult for the supervisory authority to understand and track how the personal data processing activities have been carried out. Therefore, the enforcement of the right to be forgotten can prove to be a difficult task in the metaverse.

It is important to understand that NFTs, the metaverse and blockchain technology are all concepts related to each other. It has been predicted that NFTs would be used as a currency in the metaverse. It is important to note that in the metaverse, the right to be forgotten cannot always be fully respected, especially in relation to NFTs. This is related to the technical

[41] For example, see the article by Weingarden, G. and Artzt, M. (2022) Metaverse and Privacy. *IAPP*. Available from: https://iapp.org/news/a/metaverse-and-privacy-2/; also Vittorio, A. (2022) Metaverse Technology Opens Up a Wider World of Privacy Concerns. *Bloomberg Law*. Available from: https://news.bloomberglaw.com/privacy-and-data-security/metaverse-technology-opens-up-a-wider-world-of-privacy-concerns

[42] Unknown. (2021) What is the future of your Privacy in METAverse. *Data Privacy Manager*. Available from: https://dataprivacymanager.net/what-is-the-future-of-your-privacy-in-facebook-metaverse/

functioning of NFTs and blockchain technology. Blockchain's distributed ledgers contain data that can't be deleted or changed. This means that when a data subject submits a request to have personal data deleted, this may be impossible.

If the metaverse will be a virtual universe existing in parallel to the real world, companies will not be able to exercise the same control over data processing as they can do it in the real world. If the right to be forgotten cannot be implemented in the metaverse, yet the technological development towards the metaverse is still happening at an ever-greater pace, then perhaps a political decision may be necessary here to review the current concept of the right to be forgotten and its effective exercise.

Some experts have also expressed the opinion that the metaverse can help companies to achieve greater compliance with data protection related legal acts. For example, some authors have expressed the opinion that the metaverse presents an opportunity to be a breakthrough in privacy-compliant digital marketing.[43] Indeed, it is worthwhile to note that companies have been criticized for not being able to adequately apply GDPR rules in the digital age, especially in the context of digital marketing. Companies struggle to meet all the requirements in the GDPR when carrying out digital marketing activities. Complying with all the rules in the GDPR means that digital marketing will be made less visually attractive and user-friendly. For example, users of digital platforms are overburdened with cookie consent notices and privacy policy pop-ups. Privacy notices

[43] Hiken, A. (2021) Why the metaverse could be a breakthrough in privacy-compliant digital marketing. *MarketingDive*. Available from: https://www.marketingdive.com/news/why-metaverse-could-be-breakthrough-privacy-compliant-digital-marketing/610661/. Similarly Garon, J. M. (2022) Legal Implications of a Ubiquitous Metaverse and a Web3 Future. Available from: https://ssrn.com/abstract=4002551; Di Pietro, R. and Cresci, S. (2021) Metaverse: Security and Privacy Issues. In: *Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, 13 - 15 December, Georgia: IEEE, pp. 281-288. Available from: https://ieeexplore.ieee.org/document/9750221; Wang, Y. et al. (2023) A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials* 25(1). Available from: https://ieeexplore.ieee.org/document/9880528; See also overview of privacy concerns in Metaverse Glorin, S. (2023) A Descriptive Study on Metaverse: Cybersecurity Risks, Controls, and Regulatory Framework. *International Journal of Security and Privacy in Pervasive Computing* 15(1). Available from: https://ssrn.com/abstract=4316659; Leenes emphasizing local governance Leenes, R. (2008). Privacy in the Metaverse. In: Fischer-Hübner, S., Duquenoy, P., Zuccato, A., Martucci, L. (eds) *The Future of Identity in the Information Society. Privacy and Identity 2007. IFIP — The International Federation for Information Processing* 262. Available from: https://doi.org/10.1007/978-0-387-79026-8_7; or discussion on privacy measures in Metaverse in Canbay, Y., Utku, A. and Canbay, P. (2022) Privacy Concerns and Measures in Metaverse: A Review. In: Ozbudakh, F. et al. (eds.) *15th International Conference on Information Security and Cryptography (ISCTURKEY)*, Ankara, 19 - 20 October. Turkey: ISC, pp. 80-85, Available from: https://ieeexplore.ieee.org/document/9880528

tend to be long and burdensome for data subjects to read, being full of legal terms. This has led to a situation in which data controllers are producing long privacy notices while data subjects do not bother to read them. This means that many data subjects are not even aware of their rights as data subjects, including the right to be forgotten.

The problem with long and burdensome privacy notices has already been extensively discussed by legal experts.[44] It is important to note that privacy notices have an important meaning for the right to be forgotten. A privacy notice is usually the main source of information for the data subject about its rights. According to Article 13(2)(b) and 14(2)(c) in the GDPR, it is the controller's obligation to notify the data subject about its right to request the deletion of personal data. Therefore, it is important that privacy notices are presented to a data subject in an understandable and clear way, as a privacy notice is, among its other functions, a source of information about one's right to be forgotten. Long and burdensome privacy notices are an obstacle for the effective implementation of the right to be forgotten.

Regarding the problem of long and burdensome privacy notices, some scholars have suggested that the next step is the adoption of very short 'just-in-time' contextual notices. 'Just-in-time' notices – like road signs – are there to help and can be developed in a way that blend into the right context, irrespective of whether they appear on a web page, a smartphone screen or a person's toaster display. Using "just-in-time" notices means that critical information about data processing is communicated to the data subject just before the data processing is about to take place.[45] Although such data-subject-friendly ideas have been expressed long before the idea of the metaverse came into existence, the adoption of such measures has not been very successful. Companies still publish traditional privacy notices on their webpages.

The development of the metaverse can mean that just-in-time privacy notices and other more virtual and data-subject-friendly measures may become more prevalent. This is because the metaverse means that augmented reality shall be an important part of our everyday lives. When augmented reality becomes an everyday part of our lives, controllers will be able to use augmented reality to communicate with data subjects as well. Augmented

[44] For example, see Stokel-Walker, Ch. (2022) Privacy policies are four times as long as they were 25 years ago. *New Scientist*. Available from: https://www.newscientist.com/article/2307117-privacy-policies-are-four-times-as-long-as-they-were-25-years-ago/; Delinger, A. (2019) Most privacy policies are too long and complicated to read. That needs to change. *MIC*. Available from: https://www.mic.com/impact/privacy-policies-are-too-complicated-to-understand-new-analysis-confirms-18002848.

[45] Ustaran, E. (2013) *The Future of Privacy*. London: Cecile Park Publishing, pp. 94-95.

reality enables data controllers to use images, signs and other visual aspects, instead of text, to draw data subjects' attention to changes in the processing of their personal data. These tools can be used to draw data subjects' attention to their rights, including the right to be forgotten. Therefore, there is a chance that with the help of new technology and the tools it provides, data subjects' awareness of their rights will be enhanced and subsequently offer more viable opportunities for the exercise of data subject´s rights including the right to be forgotten.

6. CONCLUSION

The expectations of forgetting in the digital age and advent of right to be forgotten were high, it is far from general regulatory success. The right to be forgotten (or its predecessor in the form of right of erasure), now stipulated in Article 17 of the GDPR, has brought with it several paradoxes. As we have seen from the case-law described in this article, in many cases, the applicants who have applied for the removal of "painful" information about themselves have become even more associated with such information. In such conditions, the right to be forgotten turns not so much into a privacy-protective instrument, but a mean of black PR on the part of both European and national courts, acting in such cases not so much as the guarantors of European justice, but as undesirable 'PR managers' for such applicants.

Aside from the Streisand effect and the Costeja paradox discussed in sections 2 and 3, the right to be forgotten also faces difficulties arising from written law itself. GDPR obliges data controllers to notify other data controllers (such as other companies) about the data erasure request as well. This can turn out to be an impossible task, especially in the digital age and unprecedent pace and speed of information flow. In the future, the right to be forgotten will face even greater challenges. The rapid development of new technologies, such as the metaverse, NFTs, blockchain technology and others will make it even more difficult for data subjects to enforce this right. On the other hand, technological advancements can also help develop innovative tools which lead to greater data protection compliance. For example, augmented reality could enable data controllers to replace long privacy notices with different visual tools which would catch the data subject's interest more efficiently.

In conclusion, the right to be forgotten plays an important role in securing data subject's rights in a world where massive amounts of information and data are being produced and processed all the time. It remains to be seen how national courts, the CJEU, data protection supervisory authorities, data

controllers as well as other key players will be able to implement this right more successfully.[46] Recent developments created some unwanted paradoxes. However, their mitigation is closely tied with important political decisions and adopting regulations in the advent of new technological development.

LIST OF REFERENCES

[1] Alessi, S. (2017) Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review* 32(1). Available from: https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1186&context=eilr

[2] Balis, J. (2022) How Brands Can Enter the Metaverse. *Harvard Business Review*. Available from: https://hbr.org/2022/01/how-brands-can-enter-the-metaverse

[3] Barbara Streisand vs. Kenneth Adelman et. al. Superior Court of California, County of Los Angeles, Case No. SC077257

[4] Bunn, A. (2015) The curious case of the right to be forgotten. *Computer Law & Security Review* 31(3). p. 336 - 350. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0267364915000606

[5] Canbay, Y., Utku, A. and Canbay, P. (2022) Privacy Concerns and Measures in Metaverse: A Review. In: Ozbudakh, F. et al. (eds.) *15th International Conference on Information Security and Cryptography (ISCTURKEY)*, Ankara, 19 - 20 October. Turkey: ISC, pp. 80-85, Available from: https://ieeexplore.ieee.org/document/9880528

[6] Charter of Fundamental Rights of the European Union (2012/C, 326/02). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT

[7] Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 3) on the Statute of the Court of Justice of the European Union, 7 June 2016 (C 202/210). Available from: http://data.europa.eu/eli/treaty/tfeu_2016/pro_3/oj

[8] Cook L. (2015) The Right to Be Forgotten: A Step in the Right Direction for Cyberspace Law and Policy. Journal of Law, Technology & Internet 6(1). Available from: https://scholarlycommons.law.case.edu/jolti/vol6/iss1/8

[46] Kocharyan, H., Hamuľák, O. and Vardanyan, L. (2022) "The Right to be Remembered?": The Contemporary Challenges of the "Streisand Effect" in the European Judicial Reality. *International and Comparative Law Review* 22(2). p. 105-120. https://doi.org/10.2478/iclr-2022-0017

[9] Cunningham, M. (2017) Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten. *Buffalo Law Review* 65(3). Available from: https://digitalcommons.law.buffalo.edu/cgi/viewcontent.cgi?article=4656&context=buffalolawreview

[10] De Baets, A. (2016) A historian's view on the right to be forgotten. *International Review of Law, Computers & Technology* 30(1-2). Available from: https://www.tandfonline.com/doi/full/10.1080/13600869.2015.1125155

[11] Delinger, A. (2019) Most privacy policies are too long and complicated to read. That needs to change. *MIC*. Available from: https://www.mic.com/impact/privacy-policies-are-too-complicated-to-understand-new-analysis-confirms-18002848

[12] Di Pietro, R. and Cresci, S. (2021) Metaverse: Security and Privacy Issues. In: *Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, 13 - 15 December, Georgia: IEEE, pp. 281-288. Available from: https://ieeexplore.ieee.org/document/9750221

[13] Erikson, P.W. (2014) The EU's right to be forgotten. Available from: https://www.linkedin.com/pulse/20140710033506-2822374-the-eu-s-right-to-be-forgotten/

[14] EU. (2022) Legal issues in the metaverse / Part 1 - Introduction to the metaverse. *CMS Legal.* Available from: https://cms-lawnow.com/en/ealerts/2022/07/legal-issues-in-the-metaverse-part-1-introduction-to-the-metaverse#:~:text=What%20is%20the%20metaverse%3F,both%2C%20e.g.%20through%20VR%20glasses.

[15] Farrall, S. et al. (eds.) (2022) *The British Journal of Criminology*, 62(6), 2022, Vol. 62, No. 6.

[16] Garon, J. M. (2022) Legal Implications of a Ubiquitous Metaverse and a Web3 Future. Available from: https://ssrn.com/abstract=4002551

[17] Giampa, G. (2016) Americans Have a Right to Be Forgotten. *Law School Student Scholarship* 740. Available from: https://scholarship.shu.edu/student_scholarship/740/

[18] Glorin, S. (2023) A Descriptive Study on Metaverse: Cybersecurity Risks, Controls, and Regulatory Framework. *International Journal of Security and Privacy in Pervasive Computing* 15(1). Available from: https://ssrn.com/abstract=4316659

[19] Google Transparency Report on delisting requests.Available from: https://transparencyreport.google.com/eu-privacy/overview.

[20] Hiken, A. (2021) Why the metaverse could be a breakthrough in

privacy-compliant digital marketing. *MarketingDive*. Available from: https://www.marketingdive.com/news/why-metaverse-could-be-breakthrough-privacy-compliant-digital-marketing/610661/

[21] Hoffman, CH. (2021) What Is the Metaverse? Is It Just Virtual Reality, or Something More? *How-to Geek*. Available from: https://www.howtogeek.com/745807/what-is-the-metaverse-is-it-just-virtual-reality-or-something-more/

[22] Holland, J.A. (2019) Contemporary Practical Alternatives to a "Right To Be Forgotten" in the United States. *Latin American Law Review* 2. Available from: https://revistas.uniandes.edu.co/doi/full/10.29263/lar02.2019.02.

[23] Hurbain v. Belgium. (2021) ECtHR, No. 57292/16.

[24] Judgement of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317,

[25] Judgement of 24 September 2019, GC and Others v. CINIL, C-136/17, EU:C:2019:773.

[26] Judgement of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, EU:C:2019:821.

[27] Keller, D. (2019) The CJEU's new filtering case, the terrorist content regulation, and the future of filtering mandates in the EU. *The Center for Internet and Society.* Available from: http://cyberlaw.stanford.edu/blog/2019/12/cjeu%E2%80%99s-new-filtering-case-terrorist-content-regulation-and-future-filtering-mandates-eu

[28] Kocharyan, H., Hamuľák, O. and Vardanyan, L. (2022) "The Right to be Remembered?": The Contemporary Challenges of the "Streisand Effect" in the European Judicial Reality. *International and Comparative Law Review* 22(2). p. 105-120. https://doi.org/10.2478/iclr-2022-0017

[29] Kulk S. and Borgesius, Z. F. (2017) Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe. In: Polonetsky, J., Tene, O. and Selinger E. (eds.) *Cambridge Handbook of Consumer Privacy*. Cambridge: Cambridge University Press. Available from: https://dare.uva.nl/search?identifier=f7d0f415-3404-426a-8833-12861fee7112

[30] Leenes, R. (2008). Privacy in the Metaverse. In: Fischer-Hübner, S., Duquenoy, P., Zuccato, A., Martucci, L. (eds) *The Future of Identity in the Information Society. Privacy and Identity 2007. IFIP — The International Federation for Information Processing* 262. Available from: https://doi.org/10.1007/978-0-387-79026-8_7.

[31] Masnick, M. (2011) Forget The Streisand Effect, I Think We've Seen The Dawning Of The Giggs Effect. *techdirt*. Available from: https://www.techdirt.com/articles/20110520/16102414365/forget-streisand-effect-i-think-weve-seen-dawning-giggs-effect.shtml.

[32] Meta. (2021) *Introducing Meta: A Social Technology Company.* [press release] 28 October. Available from: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.

[33] Mosley v. News Group Newspapers [2008] EWHC 1777 (QB).

[34] Oghia, M. J. (2018) Information Not Found: The "Right to Be Forgotten" as an Emerging Threat to Media Freedom in the Digital Age. *CIMA Digital Report*. Available from: https://www.cima.ned.org/publication/right-to-be-forgotten-threat-press-freedom-digital-age/.

[35] Opinion of AG Szpunar in Judgement of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, EU:C:2019:821.

[36] Schechner, S. (2014) Google Defends 'Right to Be Forgotten' Response. *Wall Street Journal*. Available from: https://www.wsj.com/articles/google-defends-right-to-be-forgotten-response-1416414403.

[37] Smith, M. (2019) ANALYSIS: Global Censorship, but Not Erasure, Spurs Streisand Effect. *Bloomberg Law*. Available from: https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-global-censorship-but-not-erasure-spurs-streisand-effect.

[38] Solon, O. (2014) EU 'Right To Be Forgotten' Ruling Paves Way for Censorship. *WIRED* Available at: http://www.wired.co.uk/news/archive/2014-05/13/right-to-be-forgotten-blog.

[39] Stokel-Walker, Ch. (2022) Privacy policies are four times as long as they were 25 years ago. *New Scientist*. Available from: https://www.newscientist.com/article/2307117-privacy-policies-are-four-times-as-long-as-they-were-25-years-ago/.

[40] Unknown. (2021) What is the future of your Privacy in METAverse. *Data Privacy Manager*. Available from: https://dataprivacymanager.net/what-is-the-future-of-your-privacy-in-facebook-metaverse/.

[41] Ustaran, E. (2013) *The Future of Privacy*. London: Cecile Park Publishing.

[42] Vittorio, A. (2022) Metaverse Technology Opens Up a Wider World of Privacy Concerns. *Bloomberg Law.* Available from: https://news.bloomberglaw.com/privacy-and-data-security/metaverse-technology-opens-up-a-wider-world-of-privacy-concerns

[43] W.W. v. Germany. (2018) ECtHR, No. 60798/10 and 65599/10.

[44] Wang, Y. et al. (2023) A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials* 25(1). Available from: https://ieeexplore.ieee.org/document/9880528.

[45] Weingarden, G. and Artzt, M. (2022) Metaverse and Privacy. *IAPP*. Available from: https://iapp.org/news/a/metaverse-and-privacy-2/.

[46] Wohlsen, M. (2014) For Google, the 'Right to Be Forgotten' Is an Unforgettable Fiasco. *WIRED* Available from: https://www.wired.com/2014/07/google-right-to-be-forgotten-censorship-is-an-unforgettable-fiasco/.

[47] Xue M., Magno G. et al. (2016) The Right to be Forgotten in the Media: A Data-Driven Study. *Proceedings on Privacy Enhancing Technologies 2016* (4). p. 1–14. Available from: http://www.nyu.engineering/sites/default/files/migrated/pdfs/RTBF_Data_Study.pdf

[48] Zhang, M. (2013) Beyonce Publicist's Takedown Request Causes Unflattering Photos to Go Viral. *PetaPixel*. Available from: https://petapixel.com/2013/02/08/beyonce-publicists-takedown-request-causes-unflattering-photos-to-go-viral/