DOI: https://doi.org/10.37075/EA.2024.2.11 Economic Alternatives, 2024, Issue 2, pp. 429-438

Economic Consequences of the Right to be Forgotten

Received: 15.03.2024
Available online: 30.06.2024

Jorida Xhafaj[*], Krasimir Marinov[**], Almarin Frakulli[***]

Abstract

The right to privacy and control over one's own information entails the legal right to request the removal of search results relating to one's personality if all of those results do not serve the originality of the information or the processing purposes. This paper's objective is to examine the case for a right to be forgotten from an economic standpoint and the implications of satisfying millions of requests, as well as how the General Data Protection Regulation (GDPR) has changed the way that this right is justified in society. This paper examines the economic consequences of reformulating requirements for realization and the right to remove previously classified material. The consequences are directly related to: the losses caused by a reduction in the amount of data accessible via search engines and the expected reduction in the operators' commercial interest; the way the right to be forgotten is reflected in the costs associated with processing requests; and the negative effects of violations and sanctions. The conclusions will also evaluate the effects of each search engine's obligations under the new territorial extension, as well as whether the benefits of upholding this human right outweigh all costs and efforts.

Keywords: economic costs, implications, justification, right to be forgotten.

JEL: K36, K39.

1. Introduction

Given the sensitivity of this topic and the financial impact of the collected personal data on the economic market, the data protection framework has been the subject of numerous studies in the last two decades, as technology has sophisticated. A new paradigm of stricter protection for private information has begun with the implementation of the General Data Protection Regulation (GDPR). With the intention of enhancing safeguard mechanisms in the processing and movement of personal data, and establishing consistent consumer and personal data protection across EU nations, it establishes a body of new requirements and criteria for companies that control data. So, GDPR requirements include basic information security tasks such as getting consent from subjects before processing their data, warning about information breaches, managing the exchange of information across borders in a secure way, requiring certain organizations to

[*] Law Faculty, University for Business and Technology, Kosovo
[**] Department of Marketing and Strategic Planning, University of National and World Economy
[***] Faculty of Economy, Metropolitan University of Tirana, Albania

hire an information assurance official to make sure they are following GDPR, and delisting information, which is the focus of our study.

According to Mardoff (2016), obtaining data subject consent through so-called *"clear affirmative action"* as stipulated in the Regulation has piqued the interest of users regarding the opportunity to have greater control over their data. Every legal framework that addresses restrictions or obligations, in this case pertaining to data protection, has an undeniable financial impact that is not always easily quantifiable. However, we believe that the detection of indicators that influence market economies through data processing provides us with a clearer understanding of the economic ramifications of information privacy. Particularly, we will evaluate the financial costs and benefits of the right to be forgotten, which derive from the ability to control the information about them or, due to the digital longevity, the ability to request their erasure if one of the GDPR-prescribed grounds exists.

This fundamental right is not new, and this concept is based on the notion of "self-determination" concerning "human dignity, personality, reputation, and identity," as defined by Rouvroy and Poullet (2009) and Ambrose at al., (2013). People have the right to ask search engines to take down information about them if the information is "incomplete or inaccurate" (CJEU, C-141/12 and C-372/12, 2014) and there is no reason to keep it online. Based on Article 17 of the GDPR, the data subject has the right to be forgotten through the erasure of their data, and this right has expanded the data controller's obligation to *"inform third parties that are processing such data that an erasure request has been made, and if the controller has authorized a third party to publish such personal data, the controller remains liable."* Therefore, regardless of the region in which his or her data is processed, every data subject can exercise his right to request removal of personal data (Redin, 2011). Operating on the EU market necessitates compliance with GDPR, regardless of the geographic location of the service provider or the technical means used to deliver the service.

The paper is organized in three sub-sessions to examine the changed obligations for the implementation of deletion of the past information.

Empowering the data subject to be aware of and monitor the accuracy of his personal data will have economic consequences; therefore, the primary goal of the study is to determine the economic justification of the new measures by weighing the benefits of enforcing the right to data erasure against the costs controllers will incur to ensure it. They are evaluated based on: search engine's commercial interest and the losses incurred as a result of limiting the amount of data available on online services; the balance between the positive impact on data subjects' privacy and the request processing costs; the negative financial costs faced by a controller in the event of violations and sanctions with a focus on the Regulation's stronger enforcement.

2. Methodology and approach

The present study employs a descriptive research method to describe the institution and an analytic research method to critically evaluate the effects of GDPR on the process of data delisting fulfilment as a process that necessarily involves more sophisticated infrastructure, human resources, a higher level of sanctions measures, and a direct reduction of data flow in search results. The

research also reviews the literature on the direct economic consequences of exercising the right to be forgotten under the new GDPR framework, as well as other economic consequences of search engine activity.

3. Discussion

According to Martinelli (2016), data is defined as "a catalyst for economic growth, innovation, and digitization across all economic sectors." This idea is supported especially by the new ongoing business models and the strong impact on online economic and social activities, as the strongest sidearm during the pandemic situation and afterwards. In addition, this idea is boosted by the fact that Martinelli's definition is supported by the new ongoing business models. Consequently, data has become the focal point of the knowledge economy and society, just as the European Council (Report, 2014) predicted and defined it during the development of society. In relation to this, the first phase of our research examined the link between the amount of data and the economic interest and level of impact of search engines.

Living in a "consumer data-driven and consumer data-focused commercial revolution" (Acquisti, 2010), generating data can be converted into financial incomes, particularly when used for business reasons such as e-commerce and bank transactions, market research, advertising, digital services, the creation of innovative products, or scientific studies in the health sector. Personal data, including historical data, can be converted into financial gains and traded on a market, as was already said above. As per analyst Ted Friedman (2019), "*the approach to data and analytics operations will help organizations increase the monetization of data resources"*. The first issue the research was focused on is the search engines' interest. Currently, data market enterprises place a strong emphasis on data monetization, which can lead to concrete financial benefits in the form of new data insights (analytics) or revenue from offering internet services (Newman, 2018). When used in decision-making processes or targeted advertising, data generated through business operations and the internet of things can turn customer feedback into better product design, service enhancements, organizational management, opportunity exploitation, etc. (OECD Report, 2018). Therefore, we assume that user behaviour has contributed to the increased data monetization potential, either directly or indirectly.

It is essential to note that, despite the GDPR's exclusive protection of EU citizens, its economic effects—particularly those associated with the right to be forgotten—extend far beyond the continent of Europe. First, American search engines are the most widely used worldwide, and they have already begun to modify their privacy practices and policies in order to comply with the GDPR. Second, it was confirmed in particular that the GDPR spreads its territorial reach with two types of business activities, as stated in the judgement of the European Court of Human Rights (Google Spain SL, Google Inc. v. Agencia Espanola de Protección de Datos, Mario Costeja Gonzalez (2014). Data controllers and processors outside the EU whose data processing activities are linked to offerings of goods or services to data subjects in the EU (not just EU citizens), as well as activities linked of such data subjects' behavior. As a result, these economic ventures are also subject to GDPR regulations, and the GDPR's territorial expansion affects how self-control over personal data is economically approached, resulting in data reduction.

If we pertain to the final outcomes of the study for the European Data Market, the indicators (data companies and their revenues, "*radical changes in the strategies of business' ecosystem*" (Moore, J. F. 1996), data user companies and their spending for data technologies, and the market for digital products and services) present the categories of data as a determinant of economic growth by leveraging the knowledge gleaned from predictive analytics. The study's findings suggest that "*the data economy quantifies the value of data companies by their ability to sell and produce data products and services; to establish a system developed from the use of specific problem solutions; to supply the operational infrastructure and processes that allow the company to operate and build a specific solution; and to create new jobs as a result of the use of these data products and services.*" (European Commission, 2020).

The right to one's own privacy and to exercise the autonomy over one's own data is also a property right. This approach is more prevalent in the American doctrine, where the business model based on personal data analytics has become a considerable source of data for advertising, competitiveness, innovative thinking or entrepreneurialism of new products and services. The infrastructure and service ecosystem that enables the targeting, collection, storage, and processing of personal data must adhere to GDPR and a set of standards and guidelines for the businesses should be accordingly developed.

In light of the changes, businesses must allocate resources towards developing data storage procedures, enforcing clear privacy policies, and modernizing their technology infrastructure. Continuing down the logical road of the ramifications associated to the realization of the right to be forgotten, in the second phase of our research we looked at the financial impact in relation to request processing costs that operators have to comply with.

The Recitals 65 and 66 and Special Articles of the General Data Protection Regulation, which are devoted to the data subject's right to data erasure even for past personal information relating to childhood, are examined in order to develop a comprehensive framework that fully realizes the right to self-determination in the online world. It is presumed that the right to data destruction extends not only to the controller who has made personal data public but also to the controllers who are processing the personal data to eliminate any connections, duplicates, or homologs. In this regard, it is evident that the responsibilities of data controllers and processors as outlined in the GDPR include appropriate steps, including technical and organizational measures, beginning with the design phase of any system, service, product, or process and continuing throughout their implementation. Research carried out by Nuredini et al (2022) reveals that, along with the already-existing obligations under the GDPR, companies are now subject to more duties relating to data protection, caused by the difficulties and obstacles of the worldwide economic climate, the progression of a wide range of applications, today 's evolving industries, and their resulting business model. Among the measures controllers were required to detail so that the principles of "lawfulness, fairness, and transparency" are upheld are indeed the temporary transfer of some data to a different processing system, the attempt to render some personal data inaccessible to users, and the removal of previously published web pages (Council of the European Union 2016). Within one month of receiving the request, the

organization must comply with Article 19 of the GDPR, restrict the processing of personal data, and clearly indicate this in the system.

At this point in the investigation, the required technical knowledge draws on the expertise of well-known experts who can design and implement the system capacities and solutions that allow this process step to take place. In their research analysis, Laughlin and Smouter (2018) consulted a variety of sources and professional organizations, which were largely in agreement that every organization must not only comply with practical requirements for systems but also provide a proper procedure or methodology to ensure that the data has been completely erased.

Even though the tendency towards secure automated data delisting is one of the challenges presented by the right to be forgotten, in accordance with Articles 13 and 22 of the GDPR, it is required that particular algorithmic decisions be analyzed and explained by humans. In our opinion this is a direct effect of the GDPR requirements and considering that the secure management of data delisting is still an issue that needs addressing, the idea was conceived that such restrictions will substantially increase labour costs and, according to Wallace and Castro (The Impact of the EU's New Data Protection Regulation on AI, 2018), they can compromise the "balance between accuracy and transparency".

In relation to our third argument, violations and sanctions represent the negative financial costs a controller would incur if he failed to carry out his responsibilities. The GDPR envisions an enforcement system comprised of multiple mechanisms. Therefore, administrative measures or sanctions are a system of progressive measures that are based on the seriousness of the violation or the risk of direct contravention. In addition, the GDPR makes it easier to file official complaints on behalf of individuals, an opportunity that was quickly exploited by data subjects, months after the implementation of the GDPR. One of the most discussed changes provided by the GDPR is the refreshed system of sanctions, the most severe of which can reach up to €20 million or 4% of the company's world-wide annual turnover from the prior fiscal year, whichever is significantly larger. The European Commission is authorized to implement coordinated information insurance analyses, alerts, temporary or permanent constraints of an element's capacity to process and additionally obtain information, prohibitions on processing data of EU citizens, and fines at the above levels. In addition to these categories of financial costs, we have expanded our research to include another pertinent aspect of penalties. In cases where the right to be forgotten has been violated, European courts may impose sanctions. The case of Google v. Spanish Data Protection Agency has already been mentioned, but there are numerous other cases decided by the European Court of Human Rights that fall under the violation of Article 8 of the European Convention on Human Rights. Due to the interconnectivity of this fundamental right with other recognized human rights, such as freedom of expression, national security, and public interest (Kuner at al., 2020), contentious cases are increasing in incidence. In the last five years, the European Court of Human Rights has seen an increase in the number of cases involving the right of erasure as part of the private life (Article 8 of the ECHR) and other human rights that can conflict with the right to be forgotten.

According to the ECtHR's Overview, 1959–2018 (2019), the Court found 4.83 percent of Article 8 violations in 2018, 6.55 percent in

2019, and 7 percent in 2021 during its time in operation between 1959 and the previous reporting year. Article 8 cases comprised 13% of all judgements in the previous year, or 148 out of a total of 1,105. We believe that exercising one's right to be forgotten could affect the current trend (some of the judgements are classified as key cases, and most of them confront the right to be forgotten with freedom of expression or national security).

Within our research, the possible fines have a direct economic impact on the companies dealing with personal data, but they have to be considered a high financial risk since the severity of sanction depends on criteria that are not always related to the type of breach. The data supervisor authorities in each of the EU countries responsible for administering fines are tasked with determining the objective and subjective aspects of the violation.

4. Results

Due to widespread technological complications associated with the duplication of information as a result of backups or data access from partner systems, the regulation also requires that controllers should notify and secure from partners the deletion of data at the level of a single record. Given that the efficiency of this type of resource allocation is determined by assigned responsibilities and cannot be fully observed at the time of data collection, this will undoubtedly create operational difficulties and increase the cost of operating cloud platforms.

As a result, we concur with other academics that the decrease in the quantity of personal data as a result of data erasure comprises a direct loss of benefits resulting from data analytics processes. The authors have observed an increase in delisting requests sent to search engines in the first period following the GDPR's implementation, and the significance of this effect has become clear. At that time Google alone had received 2.9% million delisting requests, with 43% of URLs meeting the delisting criteria based on the quantity of data collected (Busvine and Barzic, 2019).

The number of URLs that have recently been requested to be delisted has increased to 5,390,014 according to data from Google's transparency report (Google Transparency Report, 2023), of which 50.8% are delisted URLs. The three site types that are most frequently present on URLs requested to be delisted are news, miscellaneous, and government. At the same time, this number must be carefully considered in conjunction with the other side of the coin. In the event that a data subject's request to be removed from a list is approved, the loss of collected personal data will increase the level of data accountability. Moreover, the accountability will have a positive effect on users, as the latter will gain more control over their personal information and feel more at ease with their online behavior, thereby gaining users trust. If users are aware of their rights over personal data and the ways their rights are applied, this would reassure them of their online behavior and may encourage them to share data). Consequently, the repair effect will typically affect the compensation for the quantity of data collected from search engines. In the long term, the natural balance between what we lose and what we gain will be clearer in the relations between data subjects and search engines, which according to Waelbroeck (2018) are based on *"trust, independence of subjects, free choices of consumers, and the effect of the right to be forgotten appliance*".

Consequently, based on the analyzed provisions and enforced requirements, we believe it is indisputable that all required measures and actions for processes will be accompanied by requirements for data specialists. The execution of the majority of the delisting requests will be automated (Kaushik and Wang, Y., 2018), but the former must be overseen by a data expert who can guarantee complete deletion. Moreover, to support this argument on the economic effects of the new requirements, job opportunities for the acquisition and development of data products and services, the provision of innovative solutions, and the benefits resulting from their use will increase from 6 million in 2015 to 8.1 million in 2025 (European data market study, 2021), according to the final results of the European data market study, which measured the size and trends of the EU data economy. On the basis of this trend and a medium-term forecast, the number of data workers in Europe will increase to 10.43 million by 2020, with a compound average growth rate of 14.1%. (Martinelli, 2016).

In addition, efficiency has to be the common denominator throughout the process up to the final data delisting. We envisage the possible conduct of an audit of the organization's systems and solutions to ensure that the removal of internet links does not jeopardize the systems and solutions responsible for ensuring that the features are met and that any possible forms of intervention or new solutions do not compromise the system's integrity. The failure to comply with such a request because of technical constraints can result in an unfounded rejection of data subjects' requests. After conducting a logical regression, we can conclude that the obligations deriving from the right to be forgotten will be made specific by the introduction of the technical specifications and internal procedures that data specialists should presumably implement. This will raise costs for all organizations.

The severity and type of breach, the category of data involved, the company's track record, its willingness to cooperate with authorities to identify and resolve the issue of the offender's intent, the use of appropriate guidelines for conduct, any preventive or corrective measures taken, whether the violation was reported, and any mitigating circumstances are all taken into account (GDPR, Recitals 74-79; 82-100). Despite the fact that the GDPR has been in effect for only four years, the total amount of the twenty largest fines has reached one billion and 421,7 million euros (Data Privacy Manager, 2022). Based on fines reported by supervisory authorities from 31 European Economic Area countries during the first year, this amount has multiplied by thousands, totaling € 17,698,370 million for all 108 fines. These numbers need to be understood in the context of the other minor fines that have not been calculated and the unreported fine for violating the right to be forgotten. According to the findings of our legal analysis, there exists a distinct and severe system of penalties that will have a detrimental financial impact in the case of non-compliance with this controller's obligation. However, because individuals are more likely to trust an economic system when they see illegal behavior punished, the penalties can serve as the corrective force for stricter data privacy enforcement.

5. Conclusions

The financial effects related to the enforcement of the right to be forgotten, analyzed in this paper, can possibly involve the potential decreased amount of data for

analytics, the processing costs of the delisting requests, and the financial burden in case of legal violations of this fundamental right.

1. The decrease in the amount of personal data from the data erasure is a direct loss of benefits, which results from data analytics processes, especially considering that the right to be forgotten goes far beyond Europe, even though the GDPR only protects EU citizens. Nevertheless, the evaluation of the economic impact of the right to be forgotten appliance will be clearer in the long term of relations between data subjects and search engines, based on the trust and independence of the subjects.
2. The obligation deriving from the right to be forgotten will be specified by the introduction of necessary technical requirements and internal procedures conducted by data specialists.
3. Finally, we believe that the non-absolute character of the right to be forgotten requires that a delisting request should be evaluated on the basis of the relevant factors in each case. So, the possible violations of the right or non-fulfillment of the obligations on the part of controllers, identified in an administrative decision of supervisory authorities or in further court judgments will be converted into fines or other hefty penalties with the financial burden for the companies.

References

Acquisti, A. 2010, The Economics of Personal Data and the Economics of Privacy. Available: https://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf [Accessed 24 November 2022]

Ambrose, M. and L., Ausloos, J. 2013, The right to be forgotten across the pond. Journal of Information Policy 1(3), pp. 1–23. Doi: https://doi.org/10.5325/jinfopoli.3.2013.0001

Busvine, D.and Barzic, G., 2019, Google can limit 'right to be forgotten to EU says, top court adviser. Retrieved from https://www.reuters.com/article/us-eu-court-google/google-can-limit-right-to-be-forgotten-to-eu-adviser-to-top-court-idUSKCN1P40VJ. [Accessed 28 November 2022]

Council of the European Union 2016, Conclusions. Retrieved from: https://www.consilium.europa.eu/media/21929/15-euco-conclusions-final.pdf. [Accessed 9 February, 2023]

Data Privacy Manager, 2022. Available: https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/. [Accessed 9 September, 2022]

European Commission (2014) Towards a thriving data-driven economy, Communication from the commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions. Brussels. Available at: https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy.

European Commission 2020. Final results of the European data market study. Available at: file:///Users/mac/Desktop/edm_final_study_report_FB9B8704-C259-949F-9996ACF87CA1D054_68015.pdf. [Accessed 10 January, 2022]

European Commission 2021, Results of the new European Data Market study 2021-2023. Available at: https://digital-strategy.ec.europa.eu/en/library/results-new-european-data-market-study-2021-2023

European Commission, 2017. Final results of the European data market study measuring the size and trends of the EU data economy. Available: https://digital-strategy.ec.europa.eu/en/library/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy#:~:text=According%20to%20the%20high%20growth%20scenario%2C%20the%20value%20of%20the,%E2%82%AC%20300%20billion%20in%202016.

European Court of Human Rights, 2019. Overview 1959 – 2018 of ECtHR (2019) Available: https://www.echr.coe.int/Documents/Overview_19592018_ENG.pdf

European Data Protection Board 2019, First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities.

Farrell, J. and Shapiro, C., 2008. How Strong Are Weak Patents? *American Economic Review*, 98(4), pp. 1347-1369.

Google transparency report, 2023. Available at: https://transparencyreport.google.com/eu-privacy/overview?hl=en [Accessed 10 February, 2023]

IAPP GDPR 2019, year anniversary, Hundreds of thousands of cases and the DPOS to handle them. Available at: https://iapp.org/media/pdf/resource_center/GDPR_Anniversary_Infographic_2019.pdf

Judgment of Court of Justice of the European Union in joined Cases (2014). C-141/12 and C-372/12 YS & M and S v Minister voor Immigratie, Integratie en Asiel

Kaushik, S., Wang, Y. 2018, Data privacy: Demystifying the GDPR. Available at: https://ischool.syr.edu/infospace/2018/05/25/data-privacy-demystifying-gdpr/ [Google Scholar]

Kuner, C., Bygrave, L., Docksey, C. and Drechsler, L. (Eds.), 2020. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press. Available at: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198826491.001.0001/isbn-9780198826491 [Accessed 23 May. 2022].

Laughlin, P. and Smouter, K., 2018. How should you implement the Right to be Forgotten? Experts share best practices for dealing with customers who exercise their right to erasure. Available: https://www.mycustomer.com/marketing/data/gdpr-and-the-right-to-be-forgotten-how-to-process-requests-for-erasure. [Accessed 23 May. 2021]

Maldoff, G. 2016. Top 10 operational impacts of the GDPR: Part 3 – consent. Retrieved from https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/

Martinelli, S. 2017. Final results of the European data market study measuring the size and trends of the EU data economy.

Martinelli, S., 2019. Sharing data and privacy in the platform economy: the right to data portability and "porting rights". Regulating New Technologies in Uncertain Times, pp.133-152

Moore, J. F. 1996, The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems. HarperCollins.

Newman, M., 2018. Four models of data monetization. Retrieved from: https://inform.tmforum.org/digital-transformation-and-maturity/2018/02/four-models-data-monetization/. [Accessed 17 July, 2020].

Nuredini, B., Xhafaj, J. and Dodevska, V.P., 2022. A Comparative Overview of Data Protection in e-Commerce in the European Union, the United States of America, the

Republic of North Macedonia, and Albania: Models and Specifics. Studia Iuridica Lublinensia, 31(3), pp.61-84.

OECD, 2018. Annual report. Available: https://www.oecd.org/swac/publications/SWAC-annual-report2018_EN.pdf. [Accessed 20 December, 2019]

OECD, 2023. Emerging privacy-enhancing technologies: Current regulatory and policy approaches, *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris. Available: https://doi.org/10.1787/bf121be4-en. [Accessed 08 January, 2023]

Redin, V., 2011. Your data, your rights: Safeguarding your privacy in a connected world. Available: https://europa.eu/rapid/press-release_SPEECH-11-183_en.htm. [Accessed 20 July, 2020]

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) [2016] OJ L 119/1

Rouvroy, A. and Poullet, Y., 2009. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy.

The European court of human rights in facts and figures, 2018. Available: https://www.echr.coe.int/Documents/Facts_Figures_2018_ENG.pdf

Waelbroeck, P., 2018. Four flagships of measurement of the GDPR for the economy. Available: https://blogrecherche.wp.imt.fr/en/2018/11/14/flagship-measurements-gdpr-economy/.