International Journal of Marketing, Communication and New Media
ISSN: 2182-9306. Special Issue on Cybersecurity, Privacy, and Data Protection, FEBRUARY 2023

DOI: https://doi.org/10.54663/2182-9306.2023.sn12.42-58

Research Paper

An Analysis of Infractions and Fines in the Context of the GDPR

José Carlos Dias *
António Martins **
Pedro Pinto ***

ABSTRACT

The General Data Protection Regulation (GDPR) is the regulation that determines the directives inherent to the collection, processing, and protection of personal data in European Union (EU) countries. It was implemented in May 2018 and over the past few years, several public and private companies have been affected by serious penalties. With more than 1500 fines already registered, it is important to have an analysis and insights about them. This paper proposes a detailed analysis of the public records of fines under GDPR, understanding the average fines imposed, the main causes for their application and how they have evolved over time. It is also intended to understand the most affected sectors and point ways to mitigate these penalties. It is concluded that fines under GDPR have an increasing trend over time, both in number of fines and in value, with Industry and Commerce & Media, Telecoms and Broadcasting being the most affected sectors.

Keywords: GDPR, Fines, Penalties, Data Privacy, Infractions.

* Polytechnic Institute of Viana do Castelo, Portugal. E-Mail: djose@ipvc.pt
** Polytechnic Institute of Viana do Castelo, Portugal. E-Mail: martinsantonio@ipvc.pt
*** ADiT-LAB, Polytechnic Institute of Viana do Castelo, and INESC TEC, Portugal. E-Mail: pedropinto@estg.ipvc.pt

Received on: 2023/02/01
Approved on: 2023/02/28
Evaluated by a double-blind review system

1. INTRODUCTION

Companies collect, process, and store data about individuals, and there are many interests behind data collection, such as marketing, consumer profiling, statistical purposes, among others. Data is important to free web services, where "if something is free, you're not the customer, you are the product," as highlighted by (Schneier, 2015, p.43). Whatever the purpose, data collection and processing has become more of a reality in the life of every individual, through smartphones, computers, smartwatches, and all the other devices of daily use. As such, the importance of laws regulating their collection and processing has also become more relevant. In the same way, with the constant data collection and processing, there are also cases of fraudulent or incorrect handling of data[1]. An example of this is a few cases that have been made public.

The GDPR was implemented and made mandatory in May 2018. This regulation applies to any entity that collects, records, organizes, preserves, adapts, alters, retrieves, consults, transmits, or performs any type of operation involving personal data. This means that all entities, public or private, that process personal data are covered.

One of the most controversial cases involving data protection and personal privacy is the Facebook-Cambridge Analytica case. (J. Isaak et al., 2018; Cadwalladr et al., 2018) and it reported that data from 87 million Facebook users worldwide was collected without their consent. It is alleged that this data was used to benefit political campaigns and the case was linked to the 2018 presidential election in the United States of America.

Over the years since the GDPR implementation, several companies and entities have been hit with fines under this regulation, which already has more than 1500 fines. These numbers arouse curiosity and especially the need to understand how they have grown over time and how they are distributed across diverse infraction types, countries, and sectors of activity.

[1] https://digitalguardian.com/blog/history-data-breaches

There are already studies done on GDPR, however, most of the papers already published on the subject focus on issues such as analysis of the articles, studies of the differences between the previous rules of data protection and processing, how the GDPR affects companies economically or logistically and even make predictions of future fines.

However, there are few studies that investigate the fines already imposed, and the papers that assess the fines records make segmented analyses for specific purposes. This research aims to provide a deeper and updated analysis of all the fines imposed under the GDPR and how these are distributed across activity sectors.

This paper presents a study of the fines imposed under the GDPR, collecting, and analyzing records of these fines and observing the results.

The main objectives are understanding the average amount of the fines and how they have evolved over time, understanding which sectors of activity are most affected by the regulation, the most recurrent infractions, and the main reasons for the fines. It also highlights strategies that can be considered to mitigate this problem and ensure proper data protection and integrity. Following these objectives, three principal evaluations are the focus of this current research:

- Amount and progression of fines;
- Main activity sectors affected;
- Most common infractions and forms of mitigation.

The rest of this paper is structured as follows. Section 2 covers research on the topic, some papers related to the GDPR, those that address its application, fines, and penalties. Section 3 describes the methodology used to collect, process, and analyze the data. Section 4 describes the studies created on the collected data and the analysis of the data. Section 5 presents a discussion. Finally, Section 6 presents the conclusions.

2. RELATED WORK

A search was conducted for articles related to the topic, the keywords used in the search were “GDPR”, “fines” and “penalties”. Articles from unreliable sources and from restricted or paid sources were excluded. All articles not in English or Portuguese were also excluded. Finally, the remaining articles were analyzed based on their keywords, abstracts, and content.

Authors in (Hoofnagle et al., 2019) analyze the core points of the GDPR, explain its genesis as an extension and improvement of the 1995 Data Protection Directive, and make

predictions about the implications that the GDPR will bring. Furthermore, they provide a historical and political context for the regulation. Finally, the main concerns that the regulation brings for businesses are discussed, including the enforcement mechanism, how the GDPR presumes that activities involving data are illegal unless they have a defined basis, and the rights of data subjects. They conclude by listing the powers and tasks of Data Protection Authorities and the responsibilities of the European Data Protection Board.

In (Tikkinen-Piri et al., 2018) authors compare the Data Protection Directive 95/46/EC with the GDPR by systematically analyzing their differences and identifying the GDPR's practical implications, specifically for companies that provide services based on personal data. To summarize the results a few strategies are presented regarding the main practical implications of the changes that may aid companies to plan their actions to improve the protection of personal data and implement appropriate policies, procedures, and processes.

In (Freitas, 2018) authors address the main concerns and practical consequences of non-compliance with Directive 95/46/EC (GDPR) in Portugal. In conclusion, the aim of the article is to summarily analyze the GDPR regime regarding the protection of individuals regarding the processing of personal data and the free movement of such data.

In the paper (Calzada, 2022) authors provide a comparison between the three main global data privacy paradigms that currently exist, i.e., the General Data Protection Regulation (GDPR) in the EU, the California Consumer Privacy Act (CCPA) in the US, and the Personal Information Protection Law (PIPL) in China. In conclusion, they underline that the PIPL will clearly benefit data control by the Chinese government and allow a relevant gateway to international multilateral rules through cross-border data governance given its privileged technopolitical and geostrategic location. The aim of the article was to provide a review of the state of the art of PIPL considering the current development in the field of data privacy. As such, if the GDPR is based on fundamental rights and the CCPA is based on consumer protection, the PIPL is closely aligned with national security. Therefore, the PIPL is clearly affecting the data privacy of citizens and related stakeholders.

In the research work (Bataineh et al., 2016), the authors propose that, since personal data is constantly collected by applications and services via smartphones and networked devices, then it is possible to create a way to monetize it. The authors propose the idea of a platform where data is seen as an asset and sharing it as an economic transaction. They

suggest a model where there are data providers and customers for the data, with the central element being the management of the data and transactions.

The article (Koeninger et al., 2020) outlines the main points related to Health Insurance Portability and Accountability Act (HIPAA) and GDPR research and aims to explain how they relate, focusing on their differences and similarities. In conclusion, it indicates the necessary steps to take for compliance when these two apply.

In the article (Greenleaf et al., 2018), the authors report an increase in the number of countries that have inducted data privacy laws. They analyze the effects that the EU's GDPR is having outside Europe, and they conclude that the African continent is where this change is more significant. However, significant developments continue in Asia and South America.

The authors in (Ruohonen et al., 2022) presented a study on predicting the number of fines based on available metadata and text mining features, extracted from the documents of the enforcement decisions. It also gives a brief analysis of the most violated articles. This study uses text mining techniques, descriptive statistics, and ordinary least squares methods to answer the main research questions. They conclude by creating a model that through text and metadata mining in conjunction with regression analysis can predict GDPR infractions. The predictions are achievable with simple machine-learning techniques for regression analysis. Mean absolute errors are estimated for this model.

In the article (Wolff et al., 2021) an analysis of the 261 GDPR enforcement orders by Data Protection Authorities (DPAs) is presented during the first 2 years of GDPR implementation. In other words, the analysis goes from July 2018 to May 2020, ending up being outdated which motivates us, even more, to carry out our paper. The conclusions about this work are that regardless of addressing the main themes of the GDPR, it ends up being a bit outdated which leads to one of the conclusions being the lack of penalties regarding the transfer of data abroad or the combined processing of data. This is because it takes longer for these processes to be discovered by DPAs.

The paper (Saemann et al., 2022) analyzes 856 fines derived from the CMS Law GDPR Enforcement Tracker. It is concluded that the dataset originates from a list published by a CMS updated regularly since May 2018. It provides a basic categorization of fines based on the articles violated by the respective institution. The article enhances this category scheme by adding several subcategories that include details about the root cause, whether it was primarily a technical or organizational issue, and why the DPA initiated the

investigation. Overall, they conclude that access management turns out to be where data controllers put personal data at a higher risk.

Authors in (Georgiadis et al., 2022) reported that Big Data Analytics has improved efficiency and created many opportunities, but it has also ultimately increased the risk of personal data being compromised or breached. The General Data Protection Regulation (GDPR) enforces Data Protection Impact Assessment (DPIA) to identify appropriate controls to mitigate the risks associated with personal data protection. In conclusion, big data, specifically Big Data Analytics, can easily break the law due to the large amount of personal and sometimes sensitive data they process. Based on the authors' analysis of 159 peer-reviewed articles, they concluded that despite the large number of articles discussing the general use of privacy impact assessments, a methodology more pertinent to privacy and data protection risks in environments that store big data and apply big data analytics algorithms is still needed.

The paper (N. Gruschka et al., 2018) analyzes different data protection and privacy preservation techniques in the context of big data analysis. Furthermore, it analyzed two case studies on sensitive data and actions for complying with the data regulation laws. The first case study is a project dealing with biomedical data handling and the second is another project that concerns data collection for security operations. They further conclude that in the first project, participants were asked to give their consent to mitigate privacy concerns regarding the collection and processing of biometric data. In the second project, data from an existing data source was used and it was concluded that for projects and technologies dealing with sensitive data, a data protection impact assessment should be conducted in the initial stages of the project to identify potential privacy challenges.

The paper (Tamburri, 2020) serves to synthesize and describe the principles in the software design for GDPR. A systematic analysis of the regulation by applying the form analysis method known as Formal Concept Analysis (FCA). In conclusion, the objective of the FCA application was to elicit fundamental knowledge to drive or support the work of software engineers and designers in their campaign to design systems and redesign software in compliance with the GDPR regulation.

The article (Riva et al., 2020) examines the growing literature on methodologies for creating privacy-sensitive systems and identifies the main challenges that need to be addressed to make it easier for developers to create such systems. In conclusion, for

developers to be able to create high-tech systems with privacy in mind, practical methodologies are needed.

In the article (Kulyk, O. et al., 2020) the authors seek to answer the question "Has the GDPR hype affected users' reaction to cookie disclaimers?", the study focuses on understanding whether users' attitude towards cookie disclaimers has changed post GDPR. The authors did a study in 2017 that aimed to investigate how cookie disclaimers affect users' behavior and subsequently do this one in December 2018 to understand whether there are behavioral changes post-GDPR. The results of the study point out that there is no change in attitude towards the use of cookies, they also conclude that many users have misconceptions about their use.

In this article (Vojković et al., 2020) authors discuss the fact that the GDPR is a standardization instrument that replaces the old Data Protection Directive framework and its national transposition measures. In the context of the development of the Smart City, an analysis of the impact of evolving technological trends such as the Internet of Things, Big Data Video Surveillance and biometrics, utility payment systems, and all other types of services based on the large-scale data collection of personal data now appears. One of the main conclusions of this work is related to data controllers, as they need to ensure that the entire Smart City development process is carried out in accordance with current legal requirements through careful planning, development, and control of the functions of a Smart City. Mistakes and oversights at this stage can result in complex and costly adjustments later.

3. METHODOLOGY

There are a set of sources that provide an overview of GDPR infractions and fines. As the primary data source, it was used the GDPR Enforcement Tracker[2]. GDPR Fines Tracker and Statistics[3] source was also used to compare some records and verify the accuracy of the information. Also, it was requested a database with the source to the enforcement tracker GDPR Enforcement Tracker support team, to enable data processing, including filtering, searching, and drawing graphs of the data. The database received contained the

[2] https://www.enforcementtracker.com/
[3] https://www.privacyaffairs.com/gdpr-fines/

records from GDPR implementation until November 25, 2022. The following data were selected to be analyzed:

1. Country
2. Fine date
3. Amount
4. Sector
5. Violated articles
6. Infraction type
7. URL

Finally, the following research questions were defined to be answered by the analysis of the current research work:

1. What is the average size of a GDPR fine or penalty, and how has this changed over time?
2. What sectors have been most heavily impacted by GDPR fines and penalties?
3. What are the most common causes of GDPR fines and penalties and how can organizations avoid them?

4. AN ANALYSIS OF GDPR FINES

Figure 1 shows the total fines in euros paid in 10 countries with the most penalties. This figure shows that the amounts in this top 10 range vary from €16,232,230 to €746,273,600, with Sweden being the country with the least amount paid under the GDPR and Luxembourg being the country that paid the most. A great discrepancy is found between the first 2 countries when compared to the rest.

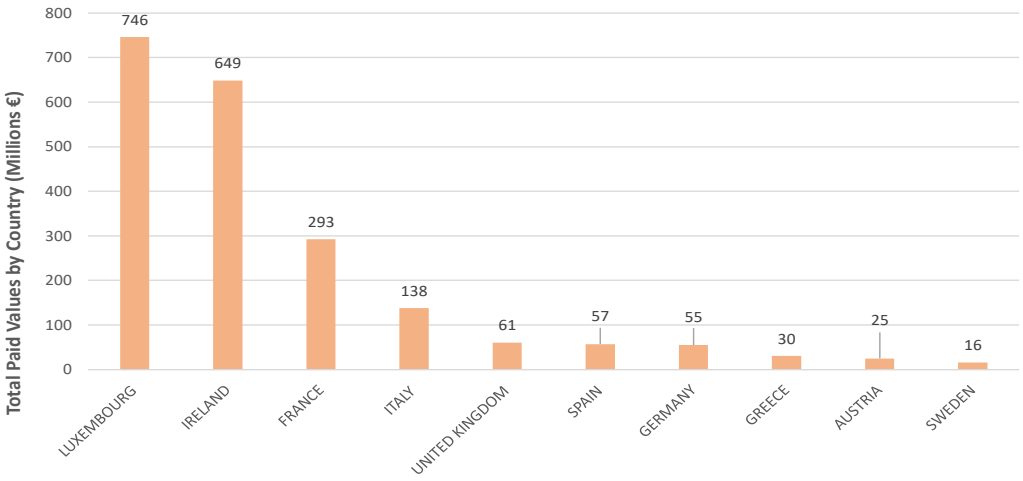

Figure 1. Countries with the highest paid values

Figure 2 presents the correlation between the number of infractions and the corresponding amount paid by the 10 most offending countries. From the results, the relationship between the number of infractions and the amounts paid seems not to be proportional. Two peculiar cases can be pointed out in this top 10, being Spain, the country with the most infractions registered and with a low amount paid in proportion. In the opposite direction, France, being only the tenth country with the most infringements, is the country that is most monetarily penalized under the GDPR.

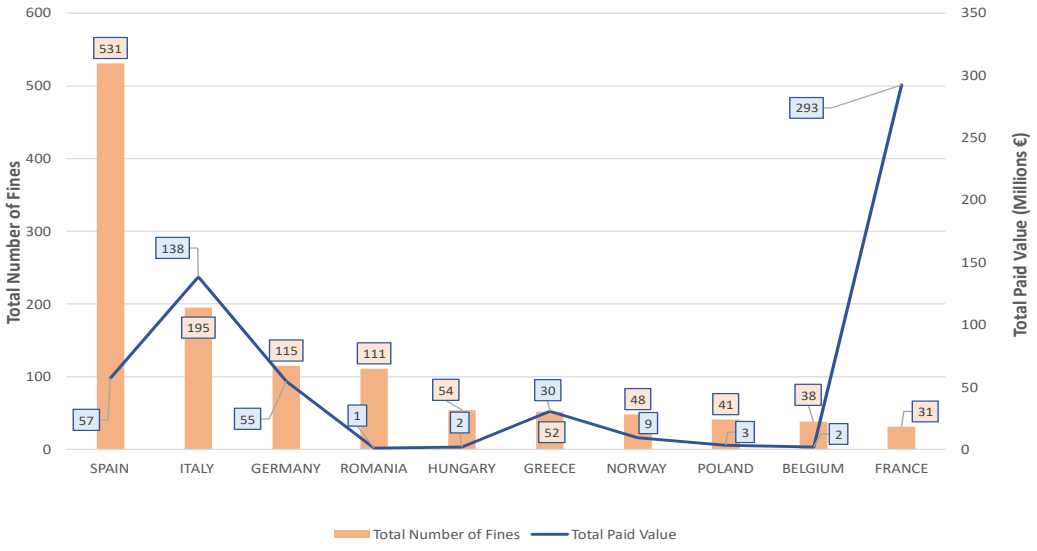

Figure 2. Correlation between total number of fines and paid value by country

4.1. Fines amount and progress

Fines under the GDPR vary widely, from hundreds of euros to hundreds of millions of euros. Figure 3 provides an overview of fines imposed under the GDPR over time. This relates the total number of fines to the total amount paid and the average amount paid, separating these statistics by year, from the implementation year of the GDPR to 2022. From these results it was excluded 20 fines with a total value of €279,376 since there was no info in which year they occurred. The results show that, although in 2022 there was a slight decrease in the number of fines, the overall trend is upward. Excluding the 2018 data which is not a full year, from 2019 to 2020 there is an increase of 212 fines, for 2021 an increase of 135 fines, which decrease by 105 for 2022.

This study also shows that the average number of fines imposed each year are:

- 2018: €38,224.00
- 2019: €436,957.87
- 2020: €453,117.89
- 2021: €2,548,966.89
- 2022: €1,364126.43

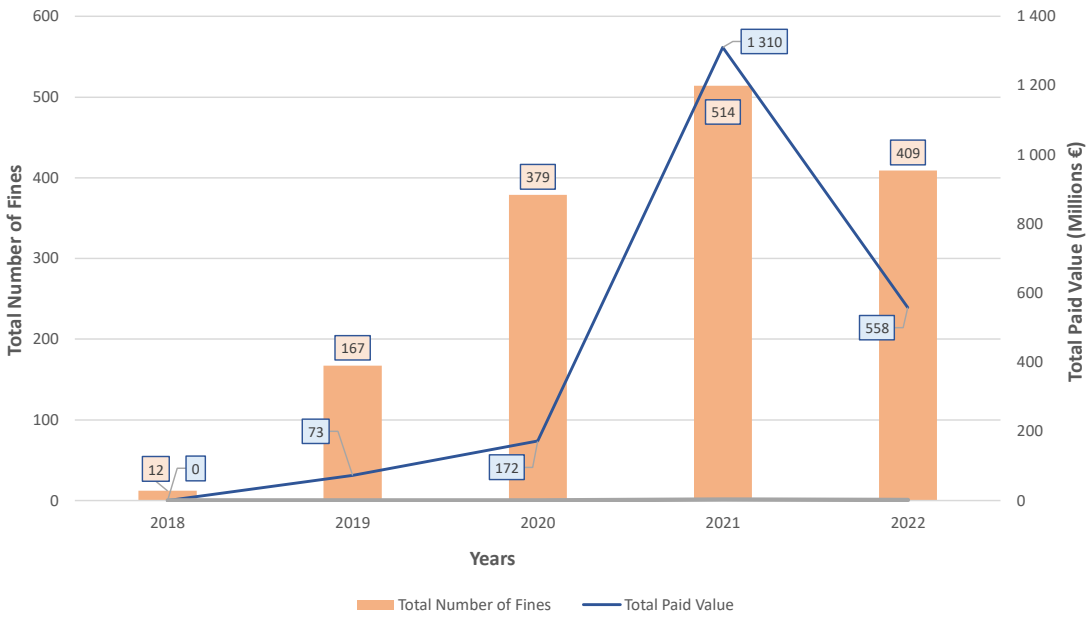

Figure 3. Evolution of fines over the years

4.2. Activity sectors

The GDPR covers sectors from Commerce to Public sector, Healthcare, Transportation and others, but there are some sectors that are more affected than others, both in terms of number of fines and amount.

Figure 4 presents the distribution of the total number of fines among the various sectors of activity and correlates it with the amount paid by each (not all sectors are presented for purposes of perceptibility). The results show that, apart from the Industry and Commerce Sector, which has the most penalties recorded, the number of infractions is evenly distributed, with no divergence standing out. It is also concluded that the Media, Telecoms and Broadcasting sector has the highest amount paid even though it is not the sector with the most infractions. It can be observed that the most affected sectors are Industry and Commerce & Media, Telecoms and Broadcasting, where it includes companies such as Vodafone España, S.A.U. being sanctioned more than 50 times, Xfera Moviles S.A., the Homeowners Association, Restaurants, Iberdrola Clients, among others. Although the number of infractions is not unreasonably higher compared to the others the monetary penalty is unparalleled.

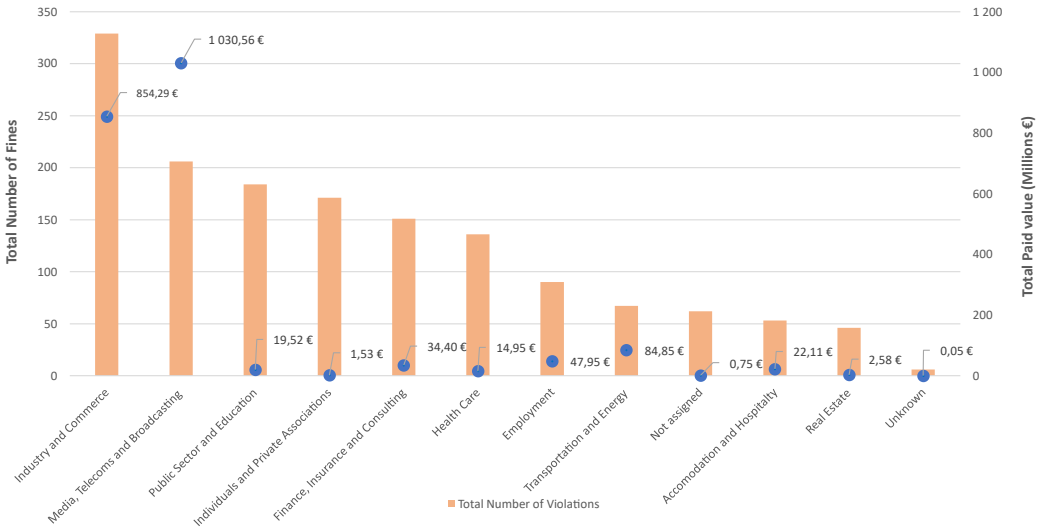

Figure 4. Correlation between number of infractions and paid value by activity sector

4.3. Common infractions and mitigations

The fines under GDPR arise for a variety of reasons according to the violated articles. Figure 5 shows the number of infractions recorded for each article. The results show that

five of the articles presented are more violated than the rest, amounting to hundreds of records. These are, in order, Art. 5, Art. 6, Art. 32, Art. 13 and Art. 12.

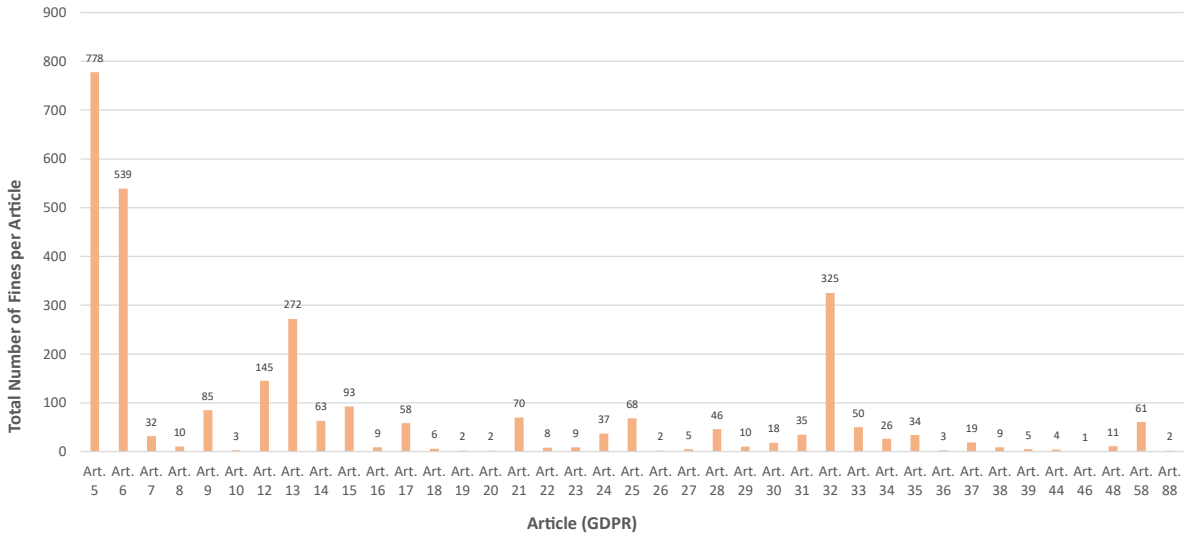

Figure 5. Total number of fines per article

Figure 6 shows the total number of infractions distributed among the distinct reasons or causes.

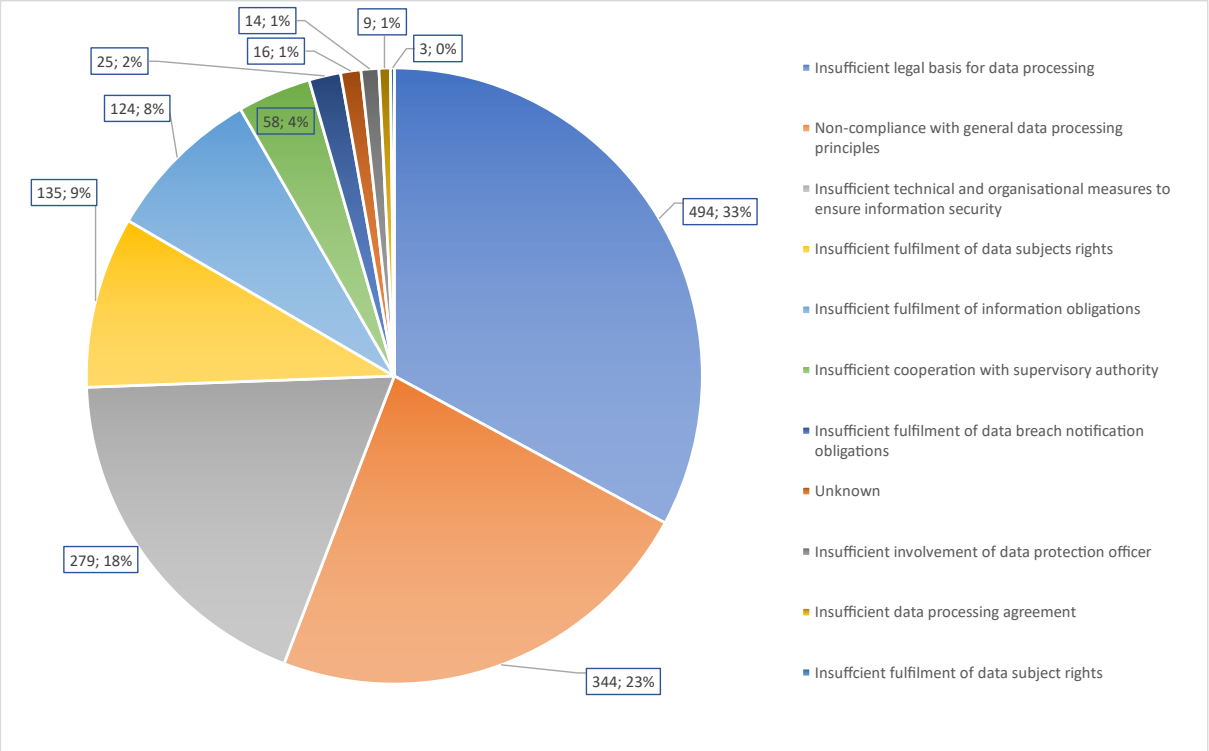

Figure 6. Distribution of fines by infraction type

The major causes fall into the following major groups of infractions:

- Insufficient legal basis for data processing;
- Non-compliance with general data processing principles;
- Insufficient technical and organizational measures to ensure information security.

An insufficient legal basis for data processing refers to a situation where an organization does not have a valid legal reason to collect, store, or use personal data. This can occur when an organization does not have the necessary consent from the individual whose data is being processed, or when the organization does not have a valid legal reason to process the data, such as a legitimate interest or legal obligation.

Non-compliance with general data processing principles refers to a situation where an organization fails to follow the basic data processing principles outlined in laws and regulations, these principles include:

- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality.

Insufficient technical and organizational measures to ensure information security refers to a situation where an organization does not have adequate safeguards in place to protect personal data from unauthorized access, disclosure, alteration, or destruction.

To mitigate these problems there are some measures that can be implemented:

- Appointing a Data Protection Officer (DPO) to support and enforce compliance with GDPR;
- Providing data subjects with clear and concise information about how their personal data is being collected, processed, and protected;
- Obtaining valid consent from data subjects before collecting or processing their personal data;
- Regularly reviewing and updating policies and procedures to ensure ongoing compliance with GDPR;
- Ensuring that any third-party processors used by the organization are also compliant with GDPR.

5. DISCUSSION

Based on the results presented, this section discusses the research questions initially proposed.

The research question "What is the average amount of a GDPR fine or penalty, and how has this changed over time?" can be answered as follows. Table 1 presents the evolution of the fines over time, in number, total and average paid value. It shows that the fines under GDPR have increased in quantity, although over the years it seems to stabilize. For now, the average fine under the GDPR is 1,364,126.43 €, although this value is influenced by the largest fines.

Table 1. Evolution of fines over time

Years	Total Number of Fines	Total Paid Value (€)	Average Paid Value (€)
2018	12	458,688.00	38,224.00
2019	167	72,971,964.00	436,957.87
2020	379	171,731,679.00	453,117.80
2021	514	1,310,168,983.00	2,548,966.89
2022	409	557,927,710.00	1,364,126.43
N/A	20	279,376.00	13,968.80

The research question "What sectors have been most heavily impacted by GDPR fines and penalties?," can be answered that the most affected sectors are Industry and Commerce & Media, Telecoms and Broadcasting, both in quantity and in value of the fines. For instance, in the top 10 most expensive GDPR fines only two do not belong to one of these two sectors. The three most expensive fines are distributed between these two sectors as follows:

1. Amazon Europe Core S.à.r.l. - (CMS process number 778) (746 million euros), Non-compliance with general data processing principles, Article: Unknown; (AMAZON.COM, INC., 2021)

2. Meta Platforms, Inc. - (CMS process number 1373) (405 million euros), Non-compliance with general data processing principles, Article: Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR; (Binding Decision, 2/2022)
3. WhatsApp Ireland Ltd. - (CMS process number 820) (225 million euros), Insufficient fulfilment of information obligations, Article: Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR. (Decision of the Data Protection Commission, 2021)

The following four fines remain in the same sectors, three of which are from Google and one from Facebook. All these are large companies with great concerns about the security and privacy of their users.

The research question "What are the most common causes of GDPR fines and penalties and how can organizations avoid them?" can be answered as follows. The fines and penalties that lead to more companies having consequences under GDPR are the insufficient legal basis for data processing, non-compliance with general data processing principles, and insufficient technical and organizational measures to ensure information security. To avoid these fines and penalties, organizations should ensure that they have valid consent mechanisms in place, have robust data protection policies and procedures in place, appoint a Data Protection Officer (DPO), and have processes in place to detect, report, and respond to data breaches promptly. Additionally, organizations should conduct regular data protection impact assessments and provide regular training to employees on data protection and privacy best practices.

The current analysis has a few limitations. All information obtained and refined through graphics and analytical studies depends on the database provided by CMS, and it assumes that this information is correct, accurate, and worthy of being used for the intended purposes. All the statistics and conclusions drawn are valid until the date of November 25th, 2022, the day of the exportation of the database on which this paper was carried out. Therefore, it is assumed that the statistics for the year 2018 are usually incomplete due to the GDPR implementation month, and the statistics for 2022 are incomplete by about a month. Given the general thrust and main objectives of the paper, these implications did not pose major problems for its realization.

6. CONCLUSIONS

The GDPR has already been implemented and is in use in the EU, and there are several articles and publications that address it in various aspects. However, it was not found any other work aimed at understanding which sectors were affected and the most recurrent causes.

This paper provides a detailed analysis of the public records of the fines issued under GDPR. This allows for understanding the average fines imposed, the main causes for their application and how they have evolved over time, and the most affected sectors of activity. From the results obtained it was found that the fines for non-compliance with the GDPR have an increasing trend, especially in the number of fines. And the most affected sectors are Industry and Commerce & Media, Telecoms and Broadcasting.

As future work and continuation of the same, it would be interesting to develop a GDPR compliance verification platform. It would work as a framework that verifies the mandatory requirements of the GDPR for each sector and indicates the items that are not being complied with according to the failures identified. Finally, after identifying the failures, the application should be able to generate automatic suggestions of corrections to be made to rectify these.

REFERENCES

Amazon.com, INC. (2021). In United States Securities and Exchange Commission (Washington, D.C. 20549). United States Securities and Exchange Commission. https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_103

Bataineh, A. S., Mizouni, R., El Barachi, M., & Bentahar, J. (2016). Monetizing personal data: a two-sided market approach. *Procedia Computer Science*, 83, 472-479.

Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR. (2022). In European Data Protection Board. edpb. https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The guardian*, 17(1), 22.

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, 5(3), 1129-1150.

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation. (2021). In European Data Protection Board (DPC Inquiry Reference: IN-18-12-2). edpb. https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf In the matter of WhatsApp Ireland Limited.

Freitas, P. M. (2018). The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint. *UNIO–EU Law Journal*, 4(2), 99-104.

Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. *Computer Law & Security Review*, 44, 105640.
Greenleaf, G., & Cottier, B. (2018). Data privacy laws and Bills: Growth in Africa, GDPR influence. GDPR Influence (April 12, 2018), 152, 11-13.
Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65-98.
J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer*, vol. 51, no. 8, pp. 56-59, August 2018, doi: 10.1109/MC.2018.3191268.
Koeninger, K., Bradshaw, R., Hinson, P. A., & Conle, J. (2020). International Health Data: How HIPAA Interacts with the EU GDPR.
Kulyk, O., Gerber, N., Hilt, A., & Volkamer, M. (2020). Has the GDPR hype affected users' reaction to cookie disclaimers?, *Journal of Cybersecurity*, 6(1).
N. Gruschka, V. Mavroeidis, K. Vishi & M. Jensen (2018). "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR", 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, pp. 5027-5033, doi: 10.1109/BigData.2018.8622621.
Riva, G. M., Vasenev, A., & Zannone, N. (2020, August). SoK: Engineering privacy-aware high-tech systems. In Proceedings of the 15th International Conference on Availability, Reliability and Security, 1-10.
Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at glance. *Information Systems*, 106, 101876.
Saemann, M., Theis, D., Urban, T., & Degeling, M. (2022). Investigating GDPR Fines in the Light of Data Flows. Proceedings on Privacy Enhancing Technologies, 4, 314-331.
Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. WW Norton & Company.
Tamburri, D. A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, 91, 101469.
Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153.
Vojković, G., & Katulić, T. (2020). *Data protection and smart cities*. Handbook of smart cities, 1-26.
Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy*, 11, 63-103.

How to cite this article:

Dias, J. C.; Martins, A.; & Pinto, P. (2023). An Analysis of Infractions and Fines in the Context of the GDPR, *International Journal of Marketing, Communication and New Media*. *Special Issue on Cybersecurity, Privacy, and Data Protection*, February 2023, 42-58.