MYKOLAS ROMERIS UNIVERSITY
LAW SCHOOL
INSTITUTE OF PRIVATE LAW

OKSANA MEZENTSEVA
EUROPEAN AND INTERNATIONAL BUSINESS LAW

# FINTECH AND THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2): A NON-DISCRIMINATION OBLIGATION ON BANKS

Master thesis

Supervisor –
Associate professor
Doctor of Laws
**Kazimieras Zaveckas**

Vilnius, 2023

**TABLE OF CONTENTS**

## LIST OF ABBREVIATIONS

**AI** - Artificial Intelligence

**AIS** - Account Information Service

**AISP** - Account Information Service Provider

**AML** - Anti-money Laundering

**API** - Application Programming Interface

**B2B** - Business-to-Business

**CJEU** - Court of Justice of the European Union

**EBA** - The European Banking Authority

**EEA** - The European Economic Area

**EU** - The European Union

**FinTech** - Financial Technology

**GDPR** - The General Data Protection Regulation

**PI** - Payment Institution

**PIS** - Payment Initiation Service

**PISP** - Payment Initiation Service Provider

**PSD1** - Directive on Payment Services in the Internal Market

**PSD2** - The Revised Payment Services Directive

**PSP** - Payments Service Provider

**PSU** - Payment Service User

**TPP** - Third Party Payment Services Provider

# INTRODUCTION

**The relevance of the master thesis.** The gradual digitalization of the world has become not only a fad of users who want to keep up with the times but also a requirement of competitiveness and solvency, coexistence in the modern world of all participants in financial relations. It is appropriate to talk about active globalization processes and a kind of erasure of the traditional concept of state borders, the existence of a single European market, which allows realizing the desire of entrepreneurs to enter new world markets to expand their business.

Also, it is impossible to ignore the requirement to modify financial relations under the rules dictated by the pandemic. All these factors have led to the emergence and development of new technologies, one of which is FinTech. The use of FinTech is now becoming an integral part of the financial services industry. Innovation and the development of information and financial technologies have increased the need to find more innovative solutions for traditional financial service providers, including banks. The main goal of FinTech is to create and operate technologies in financial law to improve the provision of services to users, including speeding up the processing of services, reducing their cost, and the ability to receive services in full and of proper quality, despite its geographical location.

Like any new technology, FinTech needs proper legal regulation to protect the rights and interests of all participants in financial relations. One of the legal instruments is PSD2 which updates and enhances the EU rules put in place by the initial PSD1 adopted in 2007. The PSD2 entered into force on 12 January 2016 and EU Member States were given until 13 January 2018 to transpose it into national law. The main objectives of the PSD2 are to contribute to a more integrated and efficient European payments market; to further level the playing field for payment service providers by including new players; to make payments safer and more secure, and to enhance protection for European consumers and businesses. In other words, the PSD2 supports innovation and competition in retail payments and enhances the security of payment transactions and the protection of consumer data.[1]

Based on our analysis of PSD2 and recent developments in FinTech, the researcher agrees with the conclusion that it can be seen as both a challenge and an opportunity to further grow the innovative business of traditional financial service providers. However, when rules do not cover

[1] European Central Bank, *The revised Payment Services Directive (PSD2) and the transition to stronger payments security*, March, 2018, Accessed April 22, 2022, URL: https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html

the whole picture, they may inadvertently discourage innovation or perhaps create barriers to innovation, closing opportunities, and competition.[2]

One of these challenges is to ensure the obligation of non-discrimination on banks during the provision of services to their client's compliance which is provided by the PSD2. Articles of the PSD2 protect PSPs from discrimination in access to the payment system; in access to accounts maintained with a credit institution; in changes in conditions of the framework contract[3]. In practice, the application of the provisions of the Directive is not sufficient and requires the simultaneous application of other legal instruments. As noted in the PSD2 guidance, The PSD2 access requirement should be read in conjunction with other legal documents. Moreover, in author's opinion, the recommendation from the PSD2 guidance: "PSPs must base their decisions about opening payment accounts for payment institutions - on an objective, non-discriminatory and proportionate assessment taking into account other legal and regulatory obligations and apply due diligence" provokes uncertain of application of non-discrimination obligation on banks[4].

During the current research devoted to the non-discrimination obligation on banks, considerable attention will be paid to the problems mentioned above of applying such obligation related to the PSPs using FinTech.

**Scientific research problem**. An analysis of the literature and legal acts related to the topic of the master's thesis indicates that there is a problem in the too narrow interpretation of PSD2 norms relating to the decision to open PSP payment accounts based on an objective, non-discriminatory and proportional assessment. PSPs, in turn, must have such access to provide payment services. As a result, this leads to the fact that traditional banking institutions create an obstacle to the development of FinTech in order to maintain their commitment among payment service consumers and prevent the formation of new FinTech participants in the market of payment services, which in turn leads to obstacles in the development of a competitive service market, which contradicts EU policies regarding competition and development of the digital market. Nevertheless, banks have the right to refuse access to accounts for PSPs and this should not be interpreted as discrimination of FinTech, for example, for the purpose of security or protection of personal data, which is regulated by relevant EU legal acts. As a result, the problem of information

[2] Inna Romānova, Simon Grima, Jonathan Spiteri, Marina Kudinska, *The Payment Services Directive II and Competitiveness: The Perspective of European FinTech Companies*, European Research Studies Journal Volume XXI, Issue 2, 2018, pp. 3 - 22.

[3] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC,* Official Journal of the European Union 337, December 23, 2015, p.35-127.

[4] European Banking Federation, *Guidance for implementation of the revised Payment Services Directive*, 2019, URL:https://www.ebf.eu/wp-content/uploads/2019/12/EBF-PSD2-guidance-Final-December-2019.pdf

sharing in private law relationships and the unique ways in which it is implemented in the area of banking law is brought up.

In light of the adoption of the PSD2, the question arises: **are the legislative instruments offered by the PSD2 sufficient to effectively regulate data-sharing issues?** The present study aims to answer this question.

**The level of the analysis of the research problem.** The research scope of the Thesis includes an analysis of the non-discrimination obligation of banks in providing payment services; a comparison of the approaches of the EU Member States to FinTech and an analysis of the main issue of the Thesis - the legal uncertainty of a non-discrimination obligation on banks applicable in FinTech.

**Review of the literature.** The main document of the thesis is PSD2 which will be analyzed for the effectiveness of anti-discriminatory behavior provisions. “Guidance for implementation of the revised Payment Services Directive” drafted by the PSD2 Expert Group of the European Banking Federation aids in a better understanding of how PSD2 regulations are really put into use as well as interaction with other legal acts. PSD2 interaction is also discussed in “EDPB Clarifies the Interplay Between GDPR and PSD2” by Niels Vandezande. The analysis of the concept of data sharing will be based on the Progress Report of the Expert Group for the Observatory on the Online Platform Economy “Work stream on Data” and Final Report “Study on data sharing between companies in Europe” which were prepared by Catarina Arnaut, Marta Pont, Elizabeth Scaria, Arnaud Berghmans, and Sophie Leconte. As for documents that are driven by EU policy on data sharing including data sharing in the private sector released by the EU Commission, “Towards a thriving data-driven economy”, “Digital Single Market Strategy”, "Free free flow of data", “Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy”, will be considered in the research Also, revision of articles dedicated to the discriminatory topic will be performed based on the following scientific works such as Jan Krämer, Daniel Schnurr, Alexandre de Streel Project Report “Internet Platforms and Non-Discrimination”, Aaron Klein "Reducing Bias in AI-based Financial Services", Darrell M West and John R Allen “TurningPoint: Policymaking in the Era of Artificial Intelligence”, Robert Bartlett, Adair Morse, Richard Stanton, Nancy Wallace “Consumer-lending Discrimination in the FinTech Era”.

**The scientific novelty of the master thesis.** Previously scholars paid attention to data sharing in providing various services in B2B relations. For example, big data presents a significant opportunity for the telecom sector to enhance internal services and the management of its infrastructure by anticipating peak usage times and figuring out how to reduce congestion, identifying clients most likely to experience billing issues, offering insights into users' decision to

leave, creating individualized offers, detecting fraud, etc.[5] Additionally, telecom operators can provide valuable information for a variety of industries, including retail, transportation, financial services, healthcare, and marketing, through the data generated by a mobile network, particularly location data. These industries can benefit from the potential of sophisticated profiling and segmentation analysis offered by enriched mobile data.[6] Nonetheless, few scholars have paid careful attention to the problem of data sharing providing payment services and non-discrimination obligations on banks among payment providers, as the adopted PSD2 also addresses this issue.

The case law of the EU Member States shows that national jurisdictions sometimes face problems concerning the question of applicable law relating to the non-discrimination obligation on banks while using payment services. This is especially relevant when banks provide their services using new technologies and innovations such as FinTech. In such a situation, it seems necessary to further study the actual problem.

**The aim of the master thesis -** is to determine the theoretical and methodological principles of FinTech activity implementation and evaluate the existing financial system in the sector of payment services with the use of FinTech.

**The objectives of the master thesis.** To achieve the goal of this master's thesis, it is necessary to perform the following tasks:

- to analyze the evolution of FinTech's application in financial relations, determine its legal nature, as well as analyze the compliance of existing legal regulations for FinTech in practice;
- to evaluate the current level of the concept of data-sharing as a part of non-discrimination duty in the private sector and how it is applicable in relation to providing payment services by banks and FinTechs in the EU;
- to develop recommendations for improving the existing financial system in the payment service field with the use of FinTech in the light of non-discriminatory obligation of banks.

**The practical significance of the master thesis.** The current research will be useful for scholars and practitioners in the field of banking law who are involved in questions about the obligations and responsibilities of banks and the performance of non-discrimination obligations in FinTech.

[5] Carol McDonald, *Big Data opportunities for Telecommunications*, November 5, 2020, Accessed April 22, 2022, URL: https://mapr.com/blog/big-data-opportunities-telecommunications/

[6] Catarina Arnaut, Marta Pont, Elizabeth Scaria, Arnaud Berghmans, Sophie Leconte, *Study on data sharing between companies in Europe*, 2018, p.6. URL: https://dl4ld.nl/KK0118016ENN.en.pdf

The master's work can also be useful for students of banking law who want to deepen their knowledge in such complex issues as the relationship between non-discrimination legislation and FinTech application legislation.

As regards the European Union policymakers, this research presents value from the perspective of possible amendments to the current EU legislation in the field of banking law, as it contains advice and suggestions for some minor but probably useful amendments to the PSD2 to make it more flexible and clear to lawyers working in the field when applying provisions of applicable substantive law in non-discrimination cases.

**The defended statements:**

- The existing level of concept on data sharing in the private sector is the key aspect of non-discrimination duty in providing payment services by banks and FinTech companies**.**
- The existing formulation of the non-discriminatory behavior of banks provided by PSD2 is not sufficient and requires interactions with numerous legal acts.

**Methods used in the master thesis.** Several methods will be used during the current scientific research.

First, one of the methods used is a historical one that allows us to understand and properly interpret the dynamic of existence and applicability of FinTech and its consideration as new and innovative technology within a time framework.

Second, one of the main methods will be the method of data collection and data analysis, due to the necessity of studying and analyzing legal texts, case law as well as scholarly articles. As a result, the collected data will be analyzed and structured and some conclusions will be deduced.

Third, since the topic of the thesis is covering data sharing issues, one of the objectives of this research is to carry out a comparative analysis to regulate this aspect under consideration. Also, various legislative acts that established the rejections and objectives of discrimination will be studied.

Also, another important scientific method is the linguistic method, which is critical in defining meaningful concepts that are used by legislators to regulate some specific issues related to the topic of the current research. This avoids unnecessary misunderstanding when analyzing various principles implemented in the texts of legislative acts and brings additional clarity to interpreting the intentions of the legislator.

Another important method that is worth mentioning is a logical method that can be seen as some kind of an interconnector between all the above-mentioned methods and allows us to make the complete vision of a problem that is subject to the current analysis and to elaborate some reasonable solutions to it.

**The structure of the master thesis.** It consists of several parts:

The first part of the master's thesis will give the concept of data sharing, its models and its importance in providing access to third-parties will be presented as a part of the non-discriminatory obligation of the bank.

In the second part, a general acknowledgment of FinTech and its applicability within the time framework and consideration of FinTech as a method for data sharing. The EU's court practices and EU legislation in the relevant area will be analyzed. Also, a comparative analysis of PSD1 and revised PSD2 on the subject of non-discrimination obligations on banks in interaction with various legislative acts will be carried out. The issue of the scope of applicable substantive law in FinTech and the measures proposed in the PSD2 will be covered.

In the third party of the study will be consider the practical significance of collaboration between FinTech and "traditional" payment institutions with an aim of developing effective competitiveness within the EU.

# 1. DATA-SHARING AND ACCESS TO THE SYSTEM AS GENERAL FUNDAMENTALS FOR NON-DISCRIMINATION

## 1.1 The Concept of Data-Sharing and its Models in B2B Sector

Businesses have previously generated and are still producing enormous amounts of data, which is continually growing. This information can boost the effectiveness of commercial services. It would be accurate to state that in today's environment, the capacity to gather, handle, analyze, and also deal with data sets is one of the elements of an enterprise's success. Therefore, businesses actively spend money on developing and implementing tools for working with data, and they also take protective measures when necessary to comply with legal requirements. The possibility of data connectivity and integration, new ideas, innovations that will drive new business opportunities, and international and cross-sector cooperation that will lead to greater efficiency in society might be some of these advantages. Open data and data sharing have the potential to improve access to and use of data, leading to advantages for both the economy and society. Examining the place of data in today's world, the commonality is defined by experts, which is to equate data with oil:

- "a new commodity spawns a lucrative, fast-growing industry, prompting antitrust regulators to step in … A century ago, the resource in question was oil"[7];
- "the world's most valuable resource is no longer oil, but data"[8];
- "data in the 21st Century is like Oil in the 18th Century: an immensely, untapped valuable asset"[9].

In contrast to the previous statements, the comparison of data is not with oil, but with water: "data as the new oil is an obsolete analogy; instead, it likened data to water as water gives life and is abundant, purified, distributed, democratic, fresh and human".[10] The researcher disagrees with this viewpoint, though, as oil provides a more tangible illustration of a product's financial benefits for both its seller and producer on the market—especially the global one. Additionally, just like with information, the use and introduction of new technologies are necessary

[7] The Economist, *The world's most valuable resource is no longer oil, but data*, May 6, 2017, Accessed April 22, 2022, URL: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[8] *Ibid*

[9] Joris Toonders, *Data Is the New Oil of the Digital Economy*, Accessed April 22, 2022, URL: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/

[10] StJohn Deakins, *Data Is The New Water: Seven Reasons Why*, October 12, 2017. Accessed April 22, 2022. URL: https://www.huffingtonpost.co.uk/stjohn-deakins-195/data-is-the-new-water-sev_b_18228184.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKFyRrFQktwDM_6MAdftvjuPQDCEadvytk8GAGhl6AwPo8yhhNIJCcRnbn-IkApnCLitJ6slcVbT6GzLikwW5Nm6VPN_XJV5Ki8729_W7Wl-w2cmnu7R5db4Enx2HkMn35LniJSB2v2eyVW-Un_lpjobXbklb0-c7RXBlQ6iwsqs

for oil and its processing. The concept that information is defined as a new oil was provided by Clive Humby: "data is the new oil, it's valuable, but if unrefined it cannot be used".[11] The author of the Thesis will concur with Clive Humby here since data processing, analysis, and subsequent application all directly affect how valuable a set of data is.

The EU Commission also mentions the potential for innovation and job development, as well as the contribution of industries across all sectors to efficiency and global competitiveness.[12] Data has become a crucial component of corporate competitiveness and their potential to contribute to innovation from an economic standpoint.[13] The findings of a 2017 study by the European Commission predicted that the value of the EU's data economy—which includes the data market, or the place where goods and services made from raw data are traded—would more than double from almost €300 billion in 2016 to €739 billion by 2020, or from €238 billion in 2016 to more than €572 billion.[14] The analysis released on July 6, 2020, lowers these estimates to value the EU's data economy in 2020 at €355 billion without the UK or €443 billion with the UK, indicating that the UK data economy alone is valued at €88 billion for the whole EU. By 2025, the EU data economy is expected to develop at a rapid rate, reaching €827 billion without the UK (or €1.036 trillion with the UK).[15] The purposeful development and funding of robots, automation, and AI are a few of the apparent causes of this increase. Additionally, consumer power plays a role in the development of a positive investment environment in the digital economy. The execution of a favorable scenario is made feasible by an open and transparent data management approach, significant innovation in the data industry, and significant data sharing. Since the provision of unhindered FinTech access to accounts is studied as part of the research, which is essentially an exchange of information, it will be appropriate to clarify what the transfer of information in the legal field is in general. This chapter analyzes the general concept of data exchange, the main models of data sharing, their features, as well as their practical application and legal regulation.

---

[11] Thomas LaRock, *"Data is the New Oil", But That Also Means it Can be Risky*, October 6, 2022, Accessed April 6, 2023, URL:https://www.dbta.com/Columns/Next-Gen-Data-Management/Data-is-the-New-Oil-But-That-Also-Means-it-Can-be-Risky155275.aspx#:~:text=British%20mathematician%20Clive%20Humby%20famously,growth%20to%20reach%20their%20goals

[12] European Commission, *Inception Impact Assessment Data Act*, Ref. Ares(2021)3527151, 28 May 2021, p. 1.

[13] Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, 2019, Luxembourg: Publications Office of the European Union, p. 76.

[14] *Embracing open data is now more important than ever (open data note 2 of 2)*, June 24, 2021, Accessed April 23, 2022, URL:https://cms-lawnow.com/en/ealerts/2021/06/embracing-open-data-is-now-more-important-than-ever-open-data-note-2-of-2

[15] The European Commission, Report/ Study The European data market study update, July 6, 2020, Accessed April 25, 2022. URL: https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update

Data is particularly obtained in three ways: by intentional sharing of data by the user (natural person or firm) of a product or service (volunteered data), by observing and capturing data automatically generated when using services or devices (observed data), and by analyzing volunteered and observed data further (inferred data). This distinction shows parallels to the different stages of data processing, starting with the collection/generation/acquisition of data, followed by their analysis (using big data analytics, etc.) and further combination/aggregation (e.g. training data) which finally allows making use of the found results, e.g. as a knowledge base or basis for (automated) decision making (AI/machine learning/deep learning).[16] The providers of services that create and generate data are private and public bodies, manufacturers of machines, and smart devices. Third parties, such as users, government agencies, other businesses that are potential competitors and non-competing businesses can and should get access to data sharing, for their further aggregation, analysis, and provision of new products and services. As a result, information providers must let third parties access their information.

Foremost, it will be appropriate to consider what open data is. The concept of "open data", represents the ability of any person to freely use, change and share non-personal data for any purpose. The Open Knowledge Foundation (OKF) defines "openness" as work:

either in the public domain or unconditionally granted a license that permits unrestricted use, redistribution, amendment (including the creation of derivative works), division (as well as the utilization, delivery, and amendment of that distinct portion of the work), the compilation (i.e. distribution with other distinct works), non-discrimination, circulation, and utilization for any objective. Provided as a whole and at no more than a reasonable one-time reproduction cost; provided in a machine-readable format where the work's elements can be easily accessed and modified; and provided in an open format with no use restrictions and capable of being fully reproduced.[17] In other words, open data is freely available information that public bodies collect, create, and financially provide. It is essential to keep in mind that not all information from the public sector is open data. The indisputable advantages of open data are the improvement of the efficiency of public services and as a consequence the improvement of public administration (for example, inter-industry data exchange); increasing social satisfaction, because information becomes more accessible and transparent; and economic growth in the private sector, contributing to the development of innovative services.

[16] Matthias Leistner, Lucie Antoine, *IPR and the use of open data and data sharing initiatives by public and private actors*, May, 2022, European Union, p.25, URL:https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf
[17] *Supra note 14*

The main legal document that regulates open data in the EU is the Open Data Directive,[18] the main aim of which is "to maximize the re-use of public data to further stimulate digital innovation in products and services, and thus to maximize social and economic benefits within the Union"[19]. The provisions of the Directive reflect key principles regarding the openness of public data and their reuse, and the most important, from the point of view of my research, is that the Directive declares that conditions for re-use for equivalent categories of re-use are non-discriminatory. Reuse requirements must be uniform for reusers and reused in similar categories. For example, different rules apply to re-use that are both commercial and non-commercial.[20] Thus, the Directive prohibits the creation of barriers and different treatment of equal categories of reuse, except for objective reasons. Subsequently, the provided prohibition of discriminatory behavior provided at the legal level for data sharing is explored.

It is reasonable to implement the concept of B2B data sharing into consideration while studying private business law. First of all, research on B2B data sharing showed that this idea is still largely unexplored and underdeveloped. Multiple terms such as data transfer and access or data sharing and re-use are being used to refer to the data sharing between businesses for commercial objectives, which might have led to misunderstandings of the idea. For this reason, the expert group of "Study on data sharing between companies in Europe" relates to the concept of B2B data sharing the supply and demand for such an exchange, while attributing to the participants both companies that provide data and those to whom such access is granted. Regarding data sharing, researchers define it as the procedure by which a firm makes its data accessible to another business that is interested in using it for commercial reasons but is neither a market rival nor a subcontractor, either for free or in exchange for payment or some other advantage. The company providing the data developed or gathered the data. As for the data reuse, the researchers defined this concept as the method through which a firm reuses data from another business for its own business needs but is not a direct rival (excluding contractor-subcontractor relationships). These data were either acquired without charge or obtained in exchange for payment or another kind of recompense, such as the delivery of a service.[21]

Repetitive use of data is the basis for forming its value in the market. In addition, re-usage dictates the release of data sets and their protection. The wide notion of incentives to share or secure data sets must be taken into account when analyzing data-sharing methods. A variety of corporate tactics for experimenting with novel judgments are used as incentives for data sharing.

---

[18] *Directive (EU) 2019/1024 of The European Parliament and of The Council of 20 June 2019 on open data and the re-use of public sector information,* Official Journal of the European Union 172, June 26, 2019, p.56-83.
[19] *Ibid, recitals 3-4, Article 1(1).*
[20] *Ibid Article 11, Recital 46.*
[21] C. Arnaut, M. Pont, E. Scaria, A. Berghmans, S. Leconte, *Study on data sharing between companies in Europe*, Luxembourg, Publications Office of the European Union p.vii; p. 2, URL:https://dl4ld.nl/KK0118016ENN.en.pdf

This can entail giving third-party businesses that don't directly work with the platform access to data in real-time. Moreover, a number of incentives for information sharing may result in direct financial benefits. Hence, while offering datasets to companies or governmental organizations. It is also appropriate to discuss the technical requirement for the functional compatibility of services as part of a comprehensive offer and fundamental service supply when taking into account the diversity of data interchange. An illustration would be commercial users of online markets having access to the platform utilizing the API. In keeping with the incentives for data interchange, some businesses share data with government agencies, research institutions, and charities for the benefit of their own reputation and the public interest.[22] Along these lines, it is confirmed that the demand for data is not primarily driven by the data itself but rather by the potential for their reuse. The technical requirements for data reuse must be followed, and the company's interests dictate the motivation for other parties to access data.

To such a degree, protection covers compliance with regulatory obligations, which may include cyber security and personal data protection. Moreover, it is also appropriate to talk about the technical component of data protection, such as protecting the service from technical responses of Disk Operating System (DOS) or restricting access during search operations. The other side of data protection is the restrictions imposed by the conduct of business, namely trade secrets, or the protection of the integrity of the core of the business model and the elimination of gap effects that form a complete offer. In addition, under certain conditions, data sharing can contribute to increasing the capabilities of dominant parties and, accordingly, increasing their dominance in the market.[23] In this regard, it is possible to conclude about the legality of the goals of the state policy to encourage the practice of data sharing, and at the same time to limit such sharing.

The Expert Group for the Observatory on the Online Platform Economy in their Progress Report "Work stream on Data" examined the modalities of data exchange, as well as different models of data sharing, which are based on a number of differences, and the nature of their distribution is characterized by a description of established practices, rather than strict recommendations:

- *One-off data sharing vs. continuous real-time access.* The debate takes place because of the right to data portability enshrined in Article 20 of the GDPR, which either provides one-time access[24] only to data or establishes a special regime for access, which is characterized by its unparalleledness, such as the obligation to access an account in accordance with the PSD2.

[22] The Expert Group for the Observatory on the Online Platform Economy, *Work stream on Data*, Accessed April 6, 2023, URL: https://platformobservatory.eu/app/uploads/2020/07/ProgressReport_Workstream_on_Data_2020.pdf
[23] *Supra note 13, p. 68, 85, 96.*
[24] *Ibid, p. 81-82.*

Thus, in accordance with PSD2, continuous access to data in real-time is established.[25] As follows, I agree with the authors that both models, one-time data exchange and continuous real-time access, are legitimate and appropriate in the application.

- *Data sharing for free or against remuneration*. The authors defined the following models of sharing since the provision of data can be as an auxiliary service or act as part of contractual obligations, and, accordingly, in this way, the data sharing takes place on a free basis. In addition, data sharing itself can be the object of business operations, as already noted earlier in this section on the economic value of information exchange. It is important to emphasize that such sharing must take place under fair, reasonable, and non-discriminatory conditions.

During the review of these models, the authors noted the abbreviation FRAND, which stands for fair, reasonable, and non-discriminatory. This concept is used to prevent a monopoly situation in cases where the owner of intellectual property rights refuses to grant a license or refuses to grant a license under FRAND terms.[26] However, John Cassels, considering what FRAND is, aptly notes that "what is fair, reasonable and non-discriminatory to one person or one context may be unfair, unreasonable and discriminatory to others in another context". As the author pointed out, the "fair" category is usually easy to identify when the license terms are truly unfair. An example is given that it is unfair to demand concessions from the licensee that is independent of the valid license agreement, such as in sales contracts, or subcontracted production; or to link the granting of a license with unrelated circumstances, i.e., what is fair, subjective and more difficult to determine. As for "reasonable", the researcher of Thesis also agrees with the author about the subjectivity of this category, but at the same time, it allows for an assessment of reasonableness and coexistence with common industry practice. And, finally, with regard to the concept of "non-discrimination", the basis here is the identification of the same treatment for all licensees who are equivalent in the same conditions. The admissibility of different treatment of licensees can be explained by the existence of an objective justification.[27] With this result, the author of Thesis agrees with the author's opinion that the exact conditions under which a FRAND will exist are not widely accepted.

- *Voluntary data sharing vs. compulsory access*. Despite the fact that data sharing is primarily voluntary, the obligation to provide access to data is established by a number of regulatory and legal acts in various areas. The CJEU has reaffirmed that "derogations from and

[25] Inge Graef, Martin Husovec, Jasper van den Boom, "*Spill-overs in data governance: Uncovering the uneasy relationship between the GDPR's right to data portability and EU sector-specific data access regimes*", Journal of European Consumer and Market Law Volume 9, Issue 1 (2020) pp. 3-16.

[26] SHIP Global IP, *FRAND licensing and why is so important for technical standards,* November 13, 2019, Accessed April 12, 2023. URL:https://shipglobalip.com/blog/frand-licensing-and-why-is-so-important-for-technical-standards-

[27] John Cassels. *What is FRAND?,* August 23, 2013, Accessed April 6, 2023, URL:https://www.fieldfisher.com/en/insights/what-is-frand

limitations on the protection of personal data must only apply in so far as is strictly necessary" and that exceptions to the directive's requirements should be based on the well-known test: when these limitations are required, appropriate, and proportionate for the reasons of national security.[28] In addition, mandatory data access is also widely used in competition protection measures. In Antea Polska, the CJEU held that EU procurement rules prevent national legislation mandating all information sent by the tenderers to the contracting authorities to be published in its entirety or communicated to the other tenderers, with the sole exception of trade secrets. The CJEU reiterated that the scope of non-disclosable information is much broader and requires a case-by-case analysis by the contracting authority, in particular with a view to avoiding the release of information that could be used to distort competition. Disclosure of information needs to strike an adequate balance between meeting good administration duties to enable the right to the effective review of procurement decisions, on the one hand, and the protection of information with commercial value or with potential competition implications, on the other.[29] In accordance with the court's decision, the researcher concluded that the opening of access to data is not an absolute right, but must serve in accordance with the balance of other private rights.

- *Data sharing with direct or indirect competitors.* Due to the necessity of legal compliance with competition requirements, competitors are obliged to exchange commercially confidential data. For this purpose, data sharing with competitors is used as a means of countering dominance and creating an effective competitive environment for all market participants. Nevertheless, in many cases, it is only possible to speak "de facto" about the general availability of data because companies can easily limit access to data, due to, for example, Google, with their terms and conditions of applications. As for indirect competitors, LinkedIn issued a stop and desist order against hiQ Labs for scraping information from the publicly accessible LinkedIn profiles posted in order to further analyze the information and offer its HR intelligence services, and hiQ Labs filed a lawsuit. The American Computer Fraud and Abuse Act of 1986 was not violated, according to the Californian court's ruling on the practice of scraping publicly accessible data (CFAA).[30] Therefore, data sharing must be done in accordance with the law, but the examples given show that companies avoid providing such access by using legal provisions.

[28] Hunton Anderws Kurth's, *CJEU Restricts Indiscriminate Access to Electronic Communications for National Security Purposes*, October 12, 2020, Accessed April 12, 2023. URL: https://www.natlawreview.com/article/cjeu-restricts-indiscriminate-access-to-electronic-communications-national-security

[29] How to Crack a Nut, *New CJEU Case Law Against Excessive Disclosure: Quid de Open Data?* (C-54/21, AND JOINED C-37/20 AND C-601/20), November 22, 2022, Accessed April 16, 2023, URL:https://www.howtocrackanut.com/blog/2022/11/22/cjeu-case-law-against-excessive-disclosure-quid-de-open-data

[30] Hudson Harris, *hiQ v. LinkedIN - Who Controls Your Publicy Available Data?*, January 7, 2018, Accessed April 12, 2023, URL: https://www.tripwire.com/state-of-security/featured/hiq-v-linkedin-controls-publicly-available-data/

- *Data portability and interoperability.* Portability is defined as the ability to transfer data from one service to another. As for interoperability, it refers to the technical features of the data infrastructure and their standardization, which determine the possibility of different technical systems interacting with each other. Both portability and interoperability occur on a voluntary basis, sometimes to comply with legal provisions such as the GDPR, PSD2, and the Digital Content Directive. Interoperability and standardization, in researcher's opinion, are truly defined by researchers as key factors for data sharing, and interoperability is defined as a condition for continuous data access in real time. The authors of the considered Report cite the Data Transfer Project as an example. Facebook, Twitter, Google, Microsoft, and Apple have developed a compatible infrastructure "with open-source code that can connect any two online service providers, enabling a seamless, direct, user-initiated portability of data between the two platforms". To access data, the Data Transfer Project makes advantage of services' already-existing APIs and permission systems. It then transfers the data into a standard format and then back into the API of the new service using service-specific adapters. The capacity to relocate one's data is a component of user control over their data on the web. Most services already allow customers to download a copy of their data, but transporting that data is still a challenge. The Data Transfer Project seeks to greatly simplify for users the process of moving data across providers.[31] The researcher can identify that the success of this project is based on the following basic principles:

- build for users means ease of finding portability tools, their easy accessibility, and comprehensibility for users. In addition, to achieve the goals of easy transfer of data between services, as well as their download, the aforementioned tools should be open and interoperable where possible with industry-standard formats;
- privacy and security are achieved due to the use of encryption technology, in order to protect against illegal access and other possibilities of acquiring data by fraudsters. Therefore, users are informed of the types and amounts of data transferred and their subsequent use by the destination service at the time the data transfer is initiated;
- reciprocity is that regardless of the user's choice to transfer data to another service, control over data should not be lost;
- focus on user data states that the data and use cases that support the individual user should be the focus of portability initiatives. Since the data people export has significance for them, focusing on the material they generate, import, approve for collection, or have influence over decreases friction for users who wish to transition between products or services or utilize their data in innovative ways. Data acquired to enhance service, such as data produced to increase system performance or train models that may be sensitive to business interests or proprietary, should not

[31] Data Transfer Initiative, Accessed April 12, 2023, URL: https://datatransferproject.dev/

be included in the scope of portability. With the knowledge that data portability regulations do not pose a danger to their unique technology, this strategy encourages businesses to continue supporting data portability;

- respect everyone, as far as people interact and share on social media, collaborate on documents, and comment on videos, photographs, and other content in our collaborative environment. Tools for data portability should only provide information that is specifically related to the individual making the transfer request[32]. Consequently, the author of the Thesis admits the point of view that it achieves the ideal mix between privacy, mobility, and the advantages of exploring a new service.

- *Data sharing when sensitive data* is concerned is seen by researchers as a separate group for discussion, as the issue of sharing such data is related to the trade-off between data protection and data security during disclosure, as studies indicate risks of re-identification of an individual even with the use of pseudo-minimization of datasets and differentiated privacy.

- *Data sharing through data markets.* Due to data sharing that can act as a commercial product in itself, specialized data markets are emerging in various industries that identify and money-oriented valuable data sets and exchanges. One such example is DAWEX, which is a data exchange platform. DAWEX market participants can share, monetize and receive data without intermediaries.[33] Due to API, the security, safety, and transparency of exchanges are managed and DAWEX functionality makes it accessible to all varieties of private companies and public-sector organizations. These organizations can coordinate the flow of data by sourcing and exchanging data securely and in accordance with applicable regulations, ensuring the integrity of license agreements.

### 1.2 Data-sharing as a Strategic Direction of the EU and its Legal Regulation

In view of common data sharing becoming frequently occurring due to a number of benefits for business development, including providing better services and increasing productivity, a number of policy initiatives and regulatory acts have been developed and issued at the EU level to regulate this area. The European Commission concluded that Europe is lagging behind the USA in its ability to leverage data opportunities, as noted in the Communication Towards a thriving data-driven Economy. In addition, it was noted that there is no financial component for research in the field of data, the complexity of the legal component, and an inadequate level of access for enterprises to large sets of data. Taking into account the proven growth potential of big data

[32] *Ibid*

[33] Data Exchange, Data Sharing, Data Marketplace & Data Hub, *Data Exchange technology for data sourcing, acquisition & sharing*, Accessed June 28, 2022, URL: https://www.dawex.com/en/

technology in a wide variety of sectors, the EU Commission emphasized the need to introduce appropriate legal support that will remove unnecessary barriers and restrictions, in order to facilitate data sharing, access to it, and the harmonization of data reuse conditions to reduce the operating costs of enterprises.[34] The author's standpoint is on account of this document, the EU initiated great progress in the development of data sharing and opened up great potential for the development of companies of the most diverse specialization. It is critical, in the researcher's opinion, that this decision was not taken earlier, despite all the obvious advantages of data sharing and the very practical necessity of adopting regulatory documents and implementing strategies for the development of such a sector. As a result, this created obstacles to the development of the data-sharing sector and reduced or completely equalized to zero the possibility of receiving any benefits from the implementation of such sharing.

In 2015, the European Commission identified the creation of a single integrated digital market as one of its main political priorities, which was stated in the Digital Single Market Strategy. With a particular emphasis on Big Data's significance, this Strategy aimed to maximize the development potential of the European Data Economy. The plan included creating a regulatory framework to address and get rid of the present obstacles and constraints to the free movement of data. The Commission recognized the transformation toward a new business environment in which knowledge, information, and data can be shared and reused in new directions. More particular, it was emphasized that a robust telecommunications sector that can dependably manage increasing volumes of data is a crucial component for making it easier for enterprises to use Big Data.[35] As follows, the purpose of the document was the optimization of the data market in the EU, namely its integration, with the aim of removing obstacles to the free exchange of data.

The "Free free flow of data" effort on the exchange of machine-generated and machine-to-machine data in a B2B setting was the next stage in the strategy. Its prerequisites were awareness of the problem of using and data sharing non-personal data created by the machine. This project aimed to address unjustifiable data location restrictions for storage or processing purposes as well as restrictions on the free flow of data for purposes other than protecting personal data.[36] The creation of innovative technologies, the requirement for their regulation, as well as their continued usage to reap additional benefits, indicate the significance of implementing this document.

---

[34] European Commission, *Towards a thriving data-driven economy*, COM (2014) 442 final, June 2, 2014, URL:http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=6210.f

[35] European Commission, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, May 6, 2015, URL:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[36] European Commission, *Free flow of non-personal data*, Accessed April 12, 2023, URL:https://digital-strategy.ec.europa.eu/en/policies/non-personal-data

The Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy[37] was produced in conjunction with the Communication on Building a European Data Economy[38] in January 2017 by the EU Commission. Both documents refer to machine-generated data, i.e., computer processes, programs, or sensors without direct human intervention. These documents declared that to develop the data economy, companies need to provide access to large and diverse data sets while respecting the provisions for the protection of personal data. In addition, it discussed restrictions on data localization that Member States impose on businesses (either through legislation or administrative decisions) that demand that certain data be stored and processed only within that particular country, and obstacles to data access and movement in B2B. In the Communication, the free flow of data throughout the EU is emphasized as a basic concept, however, it is acknowledged that data localization rules may make sense in specific situations or concerning particular data. Regarding obstacles, the Communication examines whether there are any explicit restrictions on access to and data sharing in B2B relationships. For instance, some data suppliers keep the data produced by their machines to themselves; there aren't many user-friendly tools to access and/or make data available; it's hard to determine the value of the data; or some businesses fear losing their competitive edge if their data is made available to rivals. The experts concluded that most of the time, the data is analyzed internally by the business that generates it or outsourced to analytical services. In addition, the data is not reused but instead stored internally, depriving the business of the chance to gain from data from external sources.[39] The Communication addresses new data-related challenges on responsibility, portability, interoperability, and standardization. The EU Commission emphasizes the need of resolving the responsible duties of both users and producers of data-generating devices to facilitate increased data sharing and reuse. As a result, political goals were established to solve this problem:

- access to anonymous machine-generated data should be improved;
- policies that promote data sharing, corporate investments, and assets should be protected,
- confidential data should be protected in an environment of economic competition;

[37] European Commission, *Staff Working Document on the free flow of data and emerging issues of the European data economy accompanying the Communication "Building a European data economy" (SWD(2017) 2 final), p. 25*, 2017, URL: https://ec.europa.eu/digital-single- market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy

[38] European Commission, *Building a European Data Economy*, COM(2017) 9 final January 10, 2017, URL:https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy

[39] European Commission, Directorate-General for Communications Networks, Content and Technology, Wauters, P., Siede, A., Cocoru, D., et al., *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability : final report*, Publications Office, 2018, pp. 15-16, URL:https://data.europa.eu/doi/10.2759/781960

- lock-in effects should be minimized, especially for small and medium-sized enterprises (SMEs) and start-ups.

With the release of the Data Strategy of 2020[40], the goal of establishing a Single Market for Data was further validated. This included enhancing cross-sectoral data access, use, and portability by providing a suitable data governance framework, promoting interoperability by upgrading the necessary infrastructure for hosting, processing, and using data, and developing European data spaces in strategic and public interest areas. The ideas for a Data Governance Act and a Digital Markets Act are the first examples of these more specific regulatory goals. The importance of this strategy is determined by the fact that it reflects the goal of the EU, namely the creation of a single market, including the data market. This will make it possible to significantly improve the data-sharing sector in all member countries and effectively obtain the benefits of data sharing among all participants of the single market.

Beyond a doubt, the principal legislative act regulating the sharing of data is the GDPR, which in itself is a key tool for protecting the fundamental right of individuals to protect personal data. In addition, the Regulation makes it easier for individuals to access their data and obtain information about their processing, as well as for companies, because the created one-stop-shop system creates conditions under which, in the case of cross-border data processing, companies will have to deal with only one supervisory authority.[41] In the parts that follow, the GDPR will be covered in greater detail, particularly concerning how it interacts with PSD2. However, within the scope of the subject of the section under study, it will be appropriate to consider the cases of disclosure of the third party with which information is exchanged based on the court decision of CJEU on the Right of Access to Recipients of Personal Data under GDPR. The decision was made in response to an Austrian data subject's request for an exercise of his right of access and the publication of the names of recipients of his/her personal data, which was submitted to the Austrian postal services firm. The Austrian postal services entity initially responded by outlining the reasons for processing, noting that it shared the data subject's personal information with trade partners for marketing purposes, and directing the data subject to its website for additional details. The CJEU had to consider whether Article 15 of the GDPR gave the controller the option to reveal either the categories of recipients or the precise identities of such recipients, or if it was up to the data subject to choose the level of granularity that was necessary. The CJEU concluded that in situations where personal data was provided to third parties, controllers are required to give data subjects the true

[40] European Commission, *A European strategy for data*, COM(2020) 66 final, February 19, 2020, URL: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

[41] The European Data Protection Board, *One-Stop-Shop Leaflet*, June 29, 2021, Accessed April 13, 2023. URL: https://edpb.europa.eu/our-work-tools/our-documents/one-stop-shop-leaflet_en

names of the precise recipients upon request. The CJEU claims that this reading is consistent with the GDPR's intentions and recitals. The ability of the data subject to exercise their other rights granted under the GDPR depends on their ability to exercise their right of access under Article 15 of the GDPR, which includes information on the specific recipients. The CJEU made a distinction between the controllers' duty under Articles 13 and 14 and Article 15 to reveal the recipients or categories of recipients. Meaning that controllers only have to provide information about their specific recipients upon request to exercise the right of access rather than in their privacy notices.[42] As the rights of data subjects are not absolute and should be balanced with the principle of proportionality, controllers may be excused from the requirement to reveal the identities of recipients in specific situations where it is impossible to do so, such as when it is unknown or when the requests are obviously excessive or unfounded. As a consequence, the researcher can conclude that controllers are not obliged to disclose the identity of the recipient, as the rights of data subjects are not absolute. That is, disclosure of information may not be carried out in cases where the requests are excessive or unreasonable. However, in all other cases, the controller is obliged to provide the data subject upon request with the actual identity of the recipient of his data, i.e. a third party, to exercise the right to correction, the right to limit processing, the right to erase established by the GDPR.

Another law governing data privacy in the digital environment is the nominal e-Privacy Directive. The objectives of this Directive are to protect the privacy of users of electronic communication services. The directive applies not only to telecommunications operators but also to relatively new participants in the field of electronic communications, such as Skype, Gmail, WhatsApp, Facebook Messenger, etc. The e-Privacy Directive covers content and metadata obtained from electronic communications. As both are subject to strict privacy requirements, processing them will necessitate the agreement of the data subject. Telecom companies may have greater chances to exploit data and provide extra services if private users have granted their approval.[43] This document testifies to the response of the EU legislator to the emergence and spread of new participants in the digital market, which is important because the above-mentioned companies are very popular among users, and the regulation of data-related relations when using the mentioned services is a guarantee of the protection of fundamental human rights in the digital environment.

---

[42] Judgement of the Court of Justice of 12 January 2023, *RW v Österreichische Post*, C-154/21, EU:C:2023:3, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CJ0154&from=en

[43] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, Official Journal of the European Union 201, July 31, 2002, p. 0037-0047, URL:https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

## 1.3 Summary

To put it in a nutshell, the importance of data sharing and its prospects, especially including monetary, is prevalent to derive the conclusion that the EU takes into account, accepts the challenge, develops in various aspects, trying to cover as many problematic and contentious issues as possible, makes information access easier, and benefits from the such joint use of information, which leads to adequate competition in the common single European market. This is based on an analysis of the development of policies and legal acts on the sharing of information in B2B.

The concept of "data sharing" is solely confined to the data supply side in the context of the current study thus businesses that produce or keep data and make it available to other businesses either for free or in exchange for payment, including monetary or in-kind compensation.

Private and public entities, as well as makers of machines and smart devices, supply the services that create and generate data. For the sake of additional data aggregation, analysis, and the development of new goods and services, third parties, such as users, government agencies, other businesses that are possible rivals, and non-competing enterprises, can and should be given access to data sharing. To ensure successful competition, data access must be made available to sets of aggregated competitor data.

Analyzing the legal regulation on data sharing, as well as the documents defining the strategic development of this sector, it can be concluded that when examining the functioning EU market, the actual problems are:

- incentives and data sharing initiatives;
- access to data;
- data portability with compatibility;
- technical requirements for ensuring data sharing.

In addition, the data sharing extends to the following areas of law, in particular: contract and competition law, and also raises the question of the rights of users in a certain area. Therefore, we conclude that when data is collected by a service provider, access to data must be determined at the individual level. Concerning competition, data access must be provided to sets of aggregated competitor data to establish effective competition.

## 2. THE GRANTED ACCESS TO THE BANK'S SYSTEM FOR FINTECH

### 2.1. Legal Nature of FinTech and its Role in the Exchange of Payment Data

The use of FinTech in everyday life has become so commonplace that many users do not even pay attention to the fact that it is used in everyday activities, such as payment by mobile phone in the supermarket. Additionally, FinTech is the foundation for all modern online transactions, including lending, utility payments, money transfers, and other aspects of daily life. All people all over the world now use FinTech because of its speed and convenience as well as other benefits that will be covered in the paragraphs that follow. The turning point in the development of FinTech from a newfangled technology to an everyday component of the life of an average consumer was the Covid-19 pandemic. The digitalization of all kinds of relations in society, dictated by the rules established to prevent the spread of the virus, has not bypassed financial relations. The FinTech field is expected to play a very important role in the post-COVID-19 world. And for this to happen, the FinTech industry must evolve and adapt to this new scenario.[44] Utilizing contemporary innovations, FinTech serves as a means of exchanging payment data. Clarifying what FinTech is, how it is governed by law, and how it complies with current legislation and information-sharing technologies will thus be relevant. What is more, below, arguments will be given in favor of the relevance of FinTech in the post-pandemic world.

Before all else, the researcher vehemently objects to the consideration of FinTech as a new phenomenon. To confirm this, D. W. Arner; J. Barberis; R. P. Buckley described the process of formation of FinTech in the article "The Evolution of FinTech: A New Post-Crisis Paradigm": "FinTech is not a new story, and likewise its opportunities, risks, and legal implications should not be novel. Rather, policy-makers and industry's current concerns arise not from the technology itself, but from who is applying the technology to finance and the speed of change".[45] The term's origin, however, can be traced to the early 1990s, when Citigroup established the "Financial Services Technology Consortium".[46] From their earliest stages of development, finance, and technology have been interlinked and mutually reinforcing. Finance originates in the state administrative systems that were necessary to transition from hunter-gatherer groups to settled agricultural states. For example, in Mesopotamia, written records, the earliest form of information technology, facilitated the management of administrative and economic systems, including

[44] Skeps, *The Importance of FinTech In The Post-COVID World*, June 2, 2020, Accessed May 19, 2022, URL: https://www.skeps.com/blog/the-importance-of-FinTech-in-the-post-covid-world
[45] Douglas W. Arner; Janos Barberis; Ross P. Buckley, *The Evolution of FinTech: A New Post-Crisis Paradigm*, Georgetown Journal of International Law 47, no. 4 (Summer 2016), p. 1271-1320.
[46] Paul Langley & Andrew Leyshon, *The Platform Political Economy of FinTech: Reintermediation, Consolidation and Capitalisation*, New Political Economy, 26:3,2021, p. 376-388.

through financial transactions.[47] The introduction of the telegraph with its first commercial use in 1838[48] and the laying of the first successful transatlantic cable in 1866[49] by the Atlantic Telegraph Company provided the fundamental infrastructure for the first major period of financial globalization in the late 19th century.

The first period of financial globalization, which allowed the rapid transfer of financial information across borders, was due to a combination of technology and finance and lasted until the First World War. The transfer of financial information and transactions and payments around the world were made using the telegraph, rail, canals, and steamships. Resources have been provided to develop these technologies.[50] In the post-World War I era, when financial globalization was limited for decades, technological developments, especially in the communication and information technologies used during the war, were rapid. In the context of information technology, firms such as International Business Machines (IBM) moved code-breaking tools to early computers, and Texas Instruments first released a portable financial calculator in 1967.[51] In addition, this period was characterized by the first introduction of credit cards - Diners' Club in 1950, Bank of America and American Express in 1958.[52] The beginning of the Interbank Card Association (now MasterCard) in the United States in 1966.[53] The introduction of the Automatic Teller Machine (ATM) in 1967 by Barclays Bank arguably marks the commencement of the modern evolution of today's FinTech. The ATM's impact led Paul Volcker, former chairman of the US Federal Reserve (1979-1987), to famously comment in 2009 on the role of financial innovation in the GFC of 2008: "The most important financial innovation that I have seen the past 20 years is the automatic teller machine, that helps people and prevents visits to the bank and it is a real convenience".[54]At the same time, in a short span of approximately ten years, a new strand of digital financial services in developing countries has transformed financial services availability and financial inclusion.

---

[47] Matthew Rowlinson, *Real Money and Romanticism*. Cambridge, 2010, Cambridge University Press.p.7.

[48] Giancarlo Barbiroli, *The Dynamics of Technology: a Methodological Framework for Techno-economic Analyses*, 1997, Dordrecht (Netherlands); Boston: Kluwer Academic. Theory and decisions library. Series A. Philosophy and methodology of the social science, v.25. p.317-331.

[49] Jill Hills, *The struggle for control of global communication: the formative century*, 2002, Urbana, USA University of Illinois Press.

[50] Par Dipak Dasgupta, *Financial Innovation and the State: Lessons for 21st Century Climate FinanceFrom the 19th Century Railway Era*, October 1, 2015, Accessed April 25, 2023, URL: http://www.cepii.fr/ blog/bi/ post.asp?IDcommunique 407.

[51] Patrick Thibodeau, *TI's First Handheld Calculator Is Now a Museum Piece*, September 26, 2007, Accessed April 25, 2023, URL: http://www.computerworld.com/article/2541155/computer- hardware/ti-s-first-handheld-calculator-is-now-a-museuin-piece.html.

[52] Jerry W. Markham,*From Christopher Columbus to the Robber Barons: A Financial History of the United States 1492–1900* (1st ed.), 2002, Routledge.

[53] Ben Woolsey & Emily Starbuck Gerson in *The History of Credit Cards*, May 11, 2009, Accessed April 24, 2022, URL: http://www.creditcards.com/ credit-card-news/credit-cards-history-1264.php

[54] Paul Volcker, *The Only Thing Useful Banks Have Invented in 20 Years is the ATM*, December 13, 2009, Accessed April 22, 2022, URL: http: //nypost.con/2009/12/13/the-only-thing-useful-banks-have-inivenited-ini-20-years-is-the-atm/.

D. W. Arner; J. Barberis; R. P. Buckley named FinTech the next evolutionary period as FinTech 2.0 and they defined its timely interval from 1967 to 2008 describing it as the development of traditional digital financial services. Since the beginning of this period, electronic payment systems, which are now the basis of the modern Internet and mobile payment systems, have developed rapidly, supporting both domestic and international payments and financial flows. In 1973, the Society of Worldwide Interbank Financial Telecommunications (SWIFT) was founded.[55] The subsequent collapse of Herstatt Bank in 1974 highlighted the risks of increasing international financial relationships, in particular through new payment system technology. As a result, the Basel Committee on Banking Supervision of the Bank for International Settlements (BIS) was established in 1975. This has given rise to several international soft law agreements on the development of sound payment systems and their legal regulation[56]. The Single European Act of 1986 established the framework for what would become the single financial market in the European Union. That Act, in addition to the Big Bang financial liberalization process in the United Kingdom in 1986, the 1992 Maastricht Treaty, and an ever-increasing number of financial services Directives and Regulations from the late 1980s, set the baseline for the eventual full interconnection of European Union financial markets by the early 21st Century.[57] By 1998, this process had run its full course with financial services and has become, for all practical purposes, a digital industry.[58] Risk management has become the focus of regulatory activity in the United States and Europe, on risk management of all new electronic payment systems and exchanges. As an example of regulatory interest in FinTech's developments, David Kars, then a spokesman for the Hong Kong Monetary Authority (HKMA), gave a keynote address in 1999, discussing the new regulatory framework for e-banking that has existed since 1980.[59] This delay is an illustration of that time of regulatory response to technological change. Regulating all innovations in the financial sector has limited benefits. Pre-regulation will not only increase the burden on regulators and tend to severely stifle innovation, but will also have limited benefits.[60] To sum up, this timeline reveals that the financial services sector had evolved into a mostly digital one that was dependent on electronic transactions between financial institutions, market players, and clients all over the world.

[55] *SWIFT History*, Accessed April 24, 2022, URL: https://www.swift.con/about-us/history
[56] BIS, *History of the Basel Committee, Accessed April 24*, 2022, URL: http://www.bis.org/bcbs/history.pdf.
[57] George Walker, *International Banking Regulation Law, Policy and Practice*, 2001.
[58] *Supra note 45*
[59] David Carse, *Symposium on Applied R&D: Enhancing Global Competitiveness in the Next Millennium*, October 8, 1999, URL: http://www.bis.org/review/r991012c.pdf
[60] Ravi Menon, *FinTech: Harnessing its Power, Managing its Risks*, April 2, 2016, URL: http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/FinTech-Harnessing-its-Power-Managing-its-Risks.aspx.

The regulatory view during FinTech 2.0 was that although e-banking was simply a digital version of the traditional standard banking model, it created new risks. By providing direct and virtually unrestricted access to their accounts, the technology has deprived investors of a physical presence in the withdrawal office. Indirectly, the development of e-banking can enhance e-banking, through physical interaction from withdrawals. In its activities, the ability to instantly raise funds may increase the burden on a financial institution that has liquidity problems during a crisis in the banking system.[61] Considering the current popularity of the "bank in your pocket", the author can emphasize that the introduction of electronic banking in this period was significant. Currently, it is impossible to imagine one's usual life without the use of electronic banking during everyday tasks, such as transferring funds, shopping on the Internet, paying for utilities, etc.

From 2008 to the present D. W. Arner; J. Barberis; R. P. Buckley described it as Democratizing Digital Financial Services giving the name FinTech 3.0. Public perception, regulatory control, political demand, and economic conditions are factors that have helped to level the playing field after the 2008 global financial crisis and the emergence of innovative market players and new applications of new technologies in financial services.[62] In this regard, the author of the Thesis can come to the conclusion that the legal provision of FinTech regulation accompanied it with a specific innovative technology in a specific period or raised the question of the need to introduce legal instruments that can meet all requirements and needs of all participants when using FinTech.

One of the major topics to be investigated in practical significance is there are five major conceptual frameworks for FinTech. The author can determine that these benefits are what led to its acceptance and widespread use by users:

- finance and investment - FinTech has long gone beyond crowdfunding and peer-to-peer (P2P) lending and includes funding for the technology itself.[63] For example, through mass financing, venture capital, private capital, private placement, public offerings, listing, etc. In addition to continuing the development of alternative financing mechanisms, FinTech is increasingly developing in the field of robotics consulting services;
- internal operations and risk management - the main driver of financial institutions' spending, especially since 2008, has been to provide a compliance system to cope with the sheer volume of crisis regulatory changes. As a result, the researcher can calculate FinTech's beneficial economic impact on a worldwide scale;

[61] *Supra note 45*
[62] *Ibid*
[63] Chaplius Halder & Co, Investment Advisory: The Rise of Robots, 2015, Accessed April 27, 2022, URL:http://investglass.com/images/press/Iivestmrent-Advisory-The-rise-of-the-Robots-Chappuis-Halder-InivestGlass.pdf.

- payments and infrastructure - the area of great attention of regulators since the 1970s, which led to the development of both domestic and cross-border electronic payment systems, which today are a condition for the existence of global foreign exchange markets. Similarly, the infrastructure for securities trading and settlement, as well as for Over-the-Counter (OTC) derivatives trading, remains a key aspect of the FinTech landscape and is an area where IT and telecommunications companies are looking for opportunities to abandon traditional financial institutions[64]. Implementation of innovations in the financial sector provides an opportunity to improve existing payment instruments and improve international cooperation. However, as far as the author concerned, the issue of abandoning "traditional banks" remains debatable, as their reputational position in the community is supported by a stable trust among users compared to new technologies such as Internet banking;
- data security and monetization - stability of the financial system refers to the competence of national security. The financial industry in the digital space is particularly vulnerable to cybercrime and espionage. In addition, FinTech's innovations are present in the use of big data to increase the efficiency and accessibility of financial services;
- customer interface - the main focus of traditional financial services and non-traditional developments in FinTech, which seeks to compete with traditional financial services. In other words, FinTech introduces new participants to the payment services industry, effectively fostering competition in the financial sector.

Examining the idea of FinTech and its regulatory underpinning is also required to assess FinTech as a method of data sharing. All over the world, participants in financial relations are faced with problems associated with the use of innovative technologies. And the first solution that will help reduce the number of disputes is awareness of the legal nature of FinTech and based on this introduction of the definition of FinTech at the legislative level. Recent theoretical developments of Ramona Rupeika-Apoga and Eleftherios I. Thalassinos presented in the article “Ideas for a Regulatory Definition of FinTech” have revealed that with the framework of FinTech at the international level, international organizations such as the International Monetary Fund **(**IMF), World Bank Group **(**WBG), Financial Stability Board (FSB), and others have stepped up cooperation aimed at setting guidelines for FinTech in the form of policy preparation.[65] The Bali FinTech Agenda (BFA) launched in 2008 by IMF and WBG aims to study how technological innovation is changing the delivery of financial services with results for economic efficiency and growth, financial stability, inclusion, and integrity. The BFA defines FinTech as “achieving

[64] *Supra note 45*
[65] R. Rupeika-Apoga, E. I. Thalassinos, *Ideas for a Regulatory Definition of FinTech*, International Journal of Economics and Business Administration Volume VIII, Issue 2, 2020, pp. 136-154

technologies that have the potential to transform financial services delivery by stimulating the development of new business models, applications, processes and products".[66] Moreover, The BFA is responding to calls from IMF and WBG members to expand international cooperation and make recommendations for a favorable global regulatory environment for FinTech. The FSB explains FinTech as "technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services ".[67] In 2017, the FSB published *"*Financial Stability Implications from FinTech", classifying FinTech activities that focus on the services provided, rather than suppliers or technologies used as payments, clearing and settlement; deposits, lending and capital raising; insurance; investment management; market support[68]. The Organisation for Economic Co-operation and Development (OECD) in the paper "Financial Markets, Insurance, and Private Pensions: Digitalisation and Finance" defines FinTech as "innovative applications of digital technology for financial services".[69] By criticizing definitions given by the WEF, the US National Economic Council, the FSB, the International Organization of Securities Commissions (IOSCO), the EU, and the Hong Kong Monetary Authority (HKMA), stated that "FinTech involves not only the application of new digital technologies to financial services but also the development of business models and products which rely on these technologies and more generally on digital platforms and processes".[70] The International Organization of Securities Commissions (IOSCO) defines FinTech as "a variety of innovative business models and emerging technologies that have the potential to transform the financial services industry". The IOSCO Research Report on FinTech has described eight FinTech categories: payments; insurance; planning; lending and crowdfunding; blockchain; trading and investments; data and analytics; security.[71] The main conclusion of the IMF and WBG policy paper "FinTech: the Experience so far" is that while there are important regional and national differences, countries make extensive use of FinTech capabilities to accelerate economic growth and integration while balancing risks to stability and integrity.[72] The paper "The Evolution of FinTech: A New Post-Crisis Paradigm" by Douglas W. Arner; Janos Barberis; Ross P. Buckley concludes by arguing the FinTech system provided by

[66] The Bali FinTech Agenda, *IMF Policy Paper*, October 2018, p.7.
[67] Financial Stability Board, *FinTech and market structure in financial services: Market developments and potential financial stability implications*, February 2019, Accesses April 27, 2022, URL: http://www.fsb.org/2019/02/FinTech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability- implications/.
[68] Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities*, June 27, 2017, URL: Retrieved from http://www.fsb.org/wp-content/uploads/R270617.pdf.
[69] OECD, *Financial Markets, Insurance and Private Pensions: Digitalisation and Finance*, 2018, p.3.
[70] *Ibid*, p.10.
[71] International Organisation of Securities Commissions. *IOSCO Research Report on Financial Technologies (FinTech)*, February 2017, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf.
[72] International Monetary Fund, *FinTech: the Experience so far*, IMF Policy Paper, June, 2019, p.5.

leading international organizations, concluding that the similarity of the general definition of FinTech is manifested in two ways:

- application of new/innovative technologies to financial services;
- development of new business models, applications, processes, or products based on new/innovative technologies.

The main conclusion that can be drawn is that it is unclear which technologies are new and innovative and lead to new and innovative business models and product development. The researcher's of Thesis completion of legal acts is broadly consistent with that there is no normative fixing of the FinTech definition. Notwithstanding, attention should be paid to one of the attempts to define FinTech. By doing so, in a 2017 motion for a European Parliament Resolution, the Committee on Economic and Monetary Affairs presented the report "FinTech: the Influence of Technology on the Future of the Financial Sector". In this document, the Committee established that "FinTech should be understood as finance enabled by or provided via new technologies, affecting the whole financial sector in all its components, from banking to insurance, pension funds, investment advice, payment services, and market infrastructures". Additionally, it is also proposed that "any actor can be a FinTech, regardless of the kind of legal entity it is; whereas the value chain in financial services increasingly includes alternative actors such as start-ups or tech giants; whereas this term, therefore, includes a broad range of companies and services which differ widely from one another, pose different challenges and the regulatory treatment of which has to differ".[73] Evaluating the provided definition is not legal, since this document is not legally binding, but can help in the further interpretation of the concept of FinTech when it is used.

The researcher go along with the analysis of the FinTech definition in the report "FinTech: the influence of technology on the future of the financial sector" by Carlos Goettenauer expressing in his work "FinTech: in search of a legal definition": "the report indicates that "FinTech" is not restricted to a narrow concept of financial activities. Technology has indeed impacted many-core financial activities, and in such cases, the term "FinTech" can be confidently applied. But it also reached fields that are only marginally related to the financial sector. According to the Committee of the European Parliament, the concept of FinTech ought to include even these borderline cases. The report also does not exclude incumbents from the FinTech definition. Traditional financial institutions may be considered FinTechs when they implement new technologies in the financial system. Also, tech giants can be considered relevant players in the market, as they provide infrastructure for the value chain in the financial sector".[74] The author concludes by providing a

[73] Committee on Economic and Monetary Affairs, Report on FinTech: the Influence of Technology on the Future of the Financial Sector, April 28, 2017. URL:https://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.html
[74] C. Goettenauer, *"FinTech": in search of a legal definition,* April 12, 2021, Accesses April 26, 2022, URL: https://officialblogofunio.com/2021/04/12/FinTech-in-search-of-a-legal-definition/

comprehensive concept of FinTech but expresses concern about an overly comprehensive definition.

Besides, the researcher of the Thesis would like to express her personal preference for the definition of the concept under study is the definition provided by Howell E. Jackson in his work "The Nature of the FinTech Firm and its Implications for Financial Regulation": "to define the phenomenon as encompassing a wide range of private and regulatory innovations that have become possible through the rapid decline in the cost of computing, accompanied by the widespread availability of reliable, high-speed connectivity (typically over the internet), and an explosion of newly collected data about a broad swath of personal and commercial characteristics and behaviors. This technological transformation has potentially huge implications for the domain of finance, which, to paraphrase Professors Merton and Bodie, can be helpfully demarcated as[75] "the movement of value across time and space under conditions of uncertainty that are not fully knowable by other private parties or government agents.".[76] " In addition, the author highlights the concept of "uncertainty condition" as a key one and defines what it includes: "the uncertainty whether a borrower will repay their loan, the uncertainty whether an insured risk (like an earthquake) will come to pass, the uncertainty whether providers of liquidity (like repurchase counterparties or market-makers for bonds) will withdraw unexpectedly from their markets, or the uncertainty whether interest rates will rise or fall as expected".[77] The researcher of the Thesis is of the same mind as the last scientist's point that FinTech is a more efficient and faster way to manage these and other risks (uncertainties).

Comparing the opinions of different scholars on the definition of FinTech, the author can distinguish between common and differences in their positions. It is appropriate to discuss the absence of a single agreement and, thus, a single legal definition of FinTech even if we are all discussing the regulation of the same technology. This may be explained, for example, by the uneven development of technology depending on the geographical location, the difference in national regulation of financial phenomena, and various tendencies in using financial technologies in different countries. In addition, there is a view of the rapid loss of legal definition if adopted, given the current rapid pace of technology development, which, unfortunately, is not a solution to conflicts related to the application of FinTech, and therefore, the position previously expressed on the need for legal certainty of FinTech remains a matter of debate.

Evolutionary analysis of the development and implementation of FinTech allows us to conclude about its successful use as a means of data sharing. And the search for new solutions to

[75] Howell Edmunds Jackson, The Nature of the FinTech Firm and its Implications for Financial Regulation, July 15, 2020, p.9, URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3659503
[76] Zvi Bodie, Robert C. Merton, *Finance*, 2000, Prentice Hall, 479 p.
[77] *Supra note* 75, p. 9

improve FinTech shows the further desire of users to provide payment services, that is, in the context of current research work, to exchange payment data using innovative technologies. The following stage will be to consider FinTech as a means of data sharing. The value of FinTech stems from its ability to share data in a fast, secure way among entities without any one entity having to take responsibility for safeguarding the data or facilitating the transactions. FinTech can help a lot in detecting digital payment fraud thereby enhancing the real-time exchange of transaction data and the agreement of all parties, thus eliminating fraudulent activities. When it comes to the possibility of utilizing FinTech as a channel for the sharing of data, experts view it favorably due to the properties of FinTech. Mary K. Pratt[78], for instance, concentrated on the benefits of one particular form of FinTech, and based on her research, the author of the Thesis believe that there are benefits of FinTech for businesses, including:

- trust is the most commonly cited advantage of FinTech, as its ability to secure a transaction increases the willingness of participants to enter into business relationships related to transactions or data exchange. Bitcoin and cryptocurrencies are typical examples of how FinTech provides trust between participants who do not know each other;
- decentralized structure - in addition to providing trust, which is absent in the case of a transaction between strangers, FinTech allows data to be exchanged in an ecosystem of enterprises, where no single organization is solely responsible. For example, in the case where several businesses - from suppliers and transport companies to manufacturers, distributors, and retailers - want or need information from others in this chain, but no one is responsible for facilitating the exchange of all this information. FinTech, with its decentralized nature, solves this dilemma;
- improved security and privacy - another key advantage of FinTech. It is made available owing to the technology's basic working principle: FinTech creates an immutable record of transactions with end-to-end encryption, which eliminates fraud and unauthorized activity. Moreover, it is appropriate to talk about the zero probability of hacking, since the data in FinTech is stored in a network of computers, unlike conventional computer systems that store data together on servers. Also, the best ability of FinTech to solve privacy issues is noted due to the anonymity of the data and the requirement to obtain permission to restrict access;
- reduced costs - FinTech helps businesses cut costs by eliminating the middlemen suppliers and third-party vendors that have traditionally provided the processing that FinTech can

[78] Mary K. Pratt, *Top 10 benefits of blockchain technology for business*, June 2, 2021, Accessed April 27, 2022, URL: https://www.techtarget.com/searchcio/feature/Top-10-benefits-of-blockchain-technology-for-business

do. It also reduces manual steps such as data aggregation and modification and simplifies reporting and auditing processes;

- speed - in continuation of the previous advantage, FinTech also shows significantly faster transaction processing capability due to the elimination of intermediaries and the replacement of manual transactions;
- visibility and traceability - this allows retailers to better manage inventory, respond to problems or questions, and verify the history of their items. For example, if a particular farm needs to recall its products due to contamination, a retailer using blockchain can identify and remove the products coming from that particular farm, leaving the remaining products for sale;
- immutability - a property of FinTech that prohibits the deletion or modification of transaction records. The detection technology has a timestamp and statistics for all transactions, so there is a permanent record. Thus, it can be said about the security and reliable audit of information, in contrast to the use of paper documentation and the presence of computer errors;
- individual control of data - individuals and organizations can decide which pieces of their digital data they want to share, with whom, and for how long, with limits set by smart contracts based on FinTech. This allows to talk about an unprecedented level of individual control of their digital data among users of FinTech;
- innovation - leaders across multiple industries are exploring and implementing FinTech-based systems to solve intractable problems and improve long-standing cumbersome practices.

The next argument in favor of the relevance of FinTech in the post-pandemic world is the fact that FinTech improves the profitability of financial institutions. The use of technical expertise and internal knowledge of banking systems allows for improving functions that require human intervention, among them: customer registration, security checks, payment verification, and processing. The next advantage is the possibility of personalization via big data and AI. Thanks to the development of AI technologies, financial institutions can receive, store and process an unprecedented amount of data about their customers. When handled properly, these technologies can offer customers better, more personalized financial products and services than traditional banking services. Thus, on the one hand is marketing experience, on the other hand, the client is provided with more relevant and useful information. The fact that "traditional banks" are stepping up their collaboration with FinTech at this time confirms that they must actively employ FinTech in customer service and the delivery of banking services if they hope to provide their clients the greatest experience possible and earn their loyalty.

Summarizing all of the above, the author of the Thesis come to the conclusion that FinTech is a suitable tool for the exchange of payment data. The evolutionary development of

FinTech demonstrates its prospects in further data sharing, and its advantages such as trust, decentralization, security, relatively reduced cost, speed, immutability, and individual control make FinTech not only attractive for its use by users, but also activates the cooperation of innovative technologies with "traditional banks". In addition, the appearance of new players in the form of FinTech companies on the market stimulates competition.

### 2.2 The Scope and Legal Regulation of Providing Data to the FinTech

The prevalence of the use of FinTech and its penetration into financial relations at all levels, discussed in the previous section, undoubtedly require reliable legal protection. Lawmakers have a goal to protect consumers and companies and to provide financial services in a variety of aspects at all stages of financial services. A significant breakthrough in the legal protection of individuals and groups from discrimination has not eliminated the phenomenon, which is confirmed all over the world by the fact that discriminatory acts and practices continue to take place in today's world. Discriminatory manifestations find their place in any sphere of society: education, politics, work, administration of justice, provision of social and medical services as well as payment services, etc. In addition, certain trends in society are also becoming a kind of impetus for the adoption of new regulations or improvements to existing norms. For example, much attention has been paid to the protection of personal data, which has been caused by many conflict situations due to the absence or improper application of legal provisions on consumer law. Thus, the legislator is faced with the task of implementing this human right in various relationships, including financial. Concerning financial service providers, proper legal regulation will allow effective cooperation with other institutions, and agencies, as well as the introduction of innovations and their development, which will lead to the widespread use of financial services, their investments, and other benefits. The PSD2 has many objectives aimed at improving the protection of consumers of services, stimulating innovation, and improving a level playing field for existing and new players in the field of payment services, and so on. This section will consider the prerequisites for the adoption of PSD2, the main provisions of PSD2 will also be examined, in particular in the area of prevention of discrimination, and an analysis of the compliance of legal instruments introduced by PSD2 to prevent discriminatory behavior on the part of banks will be carried out.

The predecessor of the PSD2 was the PSD1, which established the legal framework within which all EU payment service providers should operate. Before that, payment services were regulated under national rules applicable to national banks' debit schemes. Over time, they have merged with international schemes to coordinate cross-border payments. However, this has led to

inefficiencies and different interchange fees for the same service. The PSD1 aimed to create the Single Euro Payments Area (SEPA), a unique cross-border market for electronic payments - credit transfers, debit, and credit - similar to the single market for goods, capital, people, and services[79]. Despite the modest success of the PSD1 as a legal instrument, technological developments, legal gaps, and consequent legal uncertainty, as well as the need to increase cybersecurity and improve consumer protection standards, led to the revision of the PSD1. The standard solution to the problem is based on reviewing the PSD1 and adopting the PSD2 following key features:[80]

- access to payment accounts: according to the amendments, it was possible to provide access to third parties licensed to provide payment services by companies servicing the client's payment account ("PSP account maintenance"), subject to his "explicit consent". If there is evidence in the PSP of unauthorized or fraudulent activity, there is a restriction on access to the account through third-party information services. Therefore, account providers commit to "provide the means to securely communicate with account information service providers" and to facilitate their access to account information;
- liability: The European Commission has suggested that each PSP is responsible for problems with its part of the transaction, i.e. the responsibility should be shared between the service providers acting on the payer's instructions and those who receive payments on behalf of the recipients. However, when it is established that the payers acted fraudulently or with gross negligence, they are also prosecuted for unauthorized payments. However, we are interested in the fact that, for example, in the event of loss or misappropriation of a "payment instrument" such as a mobile device, the PSP should not be required to reimburse low-value unauthorized payments processed in the name of the payer;
- transparency of payments and charges: The European Commission noted that both the payer and the payee in the transaction have the right to receive information from their respective PSP about the fees applicable to the transaction. "It is important for payment service users to know the real costs and payment of payment services to make their choice," the statement said. "Accordingly, non-transparent pricing methods should not be allowed, as it is generally accepted that these methods make it extremely difficult for users to establish the real price of a payment service." Users of payment services should be entitled to information about the fee for the use of third-party payment services, which will be provided in a "clear and understandable form" before the start of payments. Recipients of payment service providers are required to provide

[79] Chikako Baba, Cristina Batog, Enrique Flores, Borja Gracia, Izabela Karpowicz, Piotr Kopyrski, James Roaf, Anna Shabunina, Rachel van Elkan, Xin Cindy Xu, *FinTech in Europe: Promises and Threats*, IMF Working Paper, November 2020.

[80] Angus McFadyen, *Key features of PSD2 and what they mean for the payments industry*, January 26, 2015, Accesses April 27, 2022, URL:https://www.pinsentmasons.com/out-law/analysis/key-features-of-psd2-and-what-they-mean-for-the-payments-industry

detailed information on the costs to be paid by recipients after payment has been made "for their services" and only if this information is available to them;

- customer authentication: modifications to the PSD2 are aimed at significantly tightening the rules for the authentication of payment service users. As a result, PSPs can be confident that the people who use their services are who they are. The Commission defines “secure client authentication” as “a procedure for verifying the identification of a natural or legal person based on the use of two or more items classified as knowledge, possession, and affiliation that are independent, as a breach of one does not compromise the reliability of others. to protect the confidentiality of authentication data". The PSP is required to "bear any financial consequences" and will be required to compensate other PSPs or intermediaries involved in the transaction, "for any losses incurred or paid" in the absence of reliable customer authentication for payments made online or by telephone if the payers themselves do not act fraudulently. In connection with the adaptation of the Commission's proposals, the PSP is obliged to use reliable customer authentication when payers access their online payment account, initiate an "electronic remote payment transaction" or "perform any actions through a remote channel that may mean the risk of payment fraud or other abuse".[81] This allows the conclusion that the key aspects of PSD2 are the establishment of rules for the licensing of payment institutions; transparency of terms and requirements for information regarding payment services, including fees; rights and obligations of users and providers of payment services; strict security requirements for electronic payments and protection of consumer financial data to ensure secure authentication and reduce the risk of fraud.[82] Thus, PSD2 facilitated access to payment accounts, established the limits of liability of participants of payment services, made clear the conditions for the provision of payment services, including their cost, and one of the most significant is the introduction of client identification, which allows increasing the security of data transmission when providing payment services. This may be considered a further validation of the PSD2 aims to ensure the further development of the integrated internal market of electronic payments in the EU, establishing comprehensive rules for payment services, to ensure harmonized rules for the provision of payment services in the EU. At the same time, PSD2 is aimed at the emergence of new participants in payment services, which will increase competition among consumers and the possibility of greater choices and better prices for them.

It will be appropriate to consider the impact of PSD1 to carry out an analysis of the evolution of ensuring the implementation of anti-discrimination provisions and subsequently to

[81] *Ibid*

[82] *Revised Rules for Payment Services in the EU*, December 6, 2021, URL:https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

provide an effective assessment of PSD2 and to conclude on the sufficiency or lack of its provisions to ensure the obligation of anti-discrimination among banks. Moreover, this section presents the legal basis of non-discriminatory bank relationships in consolidation with other acts of the Community and the close coexistence of the principle of non-discrimination, proportionality, and objectivity.

The PSD1 declared the importance of having access to the services of the technical infrastructure of payment systems, provided that they meet the requirements for ensuring the stability and integrity of these systems, that is, that they are resistant to all types of risk. In addition, it is envisaged to create conditions for non-discriminatory treatment of authorized payment institutions and credit institutions, so that any provider of payment services competing in the domestic market can use the services of the technical infrastructure of these payment systems under the same conditions. There are growing appeals for the need for equal treatment of different categories of authorized payment service providers in the Community following the terms of their licenses that have been established. In connection with this, there was an obligation to interpret the rights regarding access to the provision of payment services and access to payment systems.[83] The researcher would like to conclude that the general duty to prohibit discrimination in all spheres has been extended and legally regulated in relation to the provision of payment services under PSD1.

Based on the different prudential framework, non-identical treatment can be performed only for those authorized payment service providers and from those benefiting from a waiver not only under the The PDS1 but also under Art 8 of the Directive 2000/46/EC which is related to the electronic money institutions if the total business activities of the institution generate a total amount of financial liabilities related to outstanding electronic money that normally does not exceed EUR 5 million and never exceeds EUR 6 million; or electronic money issued by the institution is accepted as a means of payment only by any subsidiaries of the institution that perform operational or other support functions; or electronic money issued by the institution is accepted as payment only by a limited number of businesses that can be clearly distinguished by: their location in the same area; or their close financial or business relationship with the issuing institution, such as a marketing or distribution scheme.[84] The PSD1 also states that any differential treatment regarding pricing policy only takes place if motivated by differences in costs caused by payment service providers.

---

[83] *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance)*, Official Journal of the European Union, December 5, 2007, p. 1-36**,** Recital 19

[84] *Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions*, Official Journal of the European Union, October 27, 2000, p.0039-0043, Article 8

Article 28 of the PSD1 established access to the payment systems in a non-discriminatory manner for authorized or registered payment services. It also mentions the objectivity and proportionality of access to payment systems, which can be limited only because of operational and business risks, as well as to protect the financial and operational stability of the payment system. In addition, Paragraph 1 of the article in question also prohibits the establishment of any rule that will limit the effective participation in other payment systems for providers of payment services, their users, and other payment systems. It once again emphasized the prohibition of establishing any rule that is discriminatory concerning authorized payment service providers or registered payment service providers regarding the rights, obligations, and rights of participants. Any restrictions based on institutional status are also prohibited.

Regarding the exceptions to the application of Article 28 of the PSD1, the second paragraph provides:

- payment systems designating by Directive 98/26/EC;
- payment systems, which include providers of payment services that are part of a group that includes organizations related to capital, and one of the entities has significant control over other entities of this organization;
- payment systems represented by a single provider of payment services, which can be an individual or a group, in the event that such a participant acts or can be a provider of payment services for both the payer and the recipient, and his competence includes the exclusive responsibility for managing the system and presents licenses to other payment service providers to participate in the system, and such payment service providers do not have the competence to negotiate fees among themselves for the payment system, but they can set their prices for payers and payees.[85]

Considering provisions of non-discrimination that were declared by Article 44 of the PSD1, it was also mentioned the prohibition of discriminatory manner for payment service users while changes in the interest or exchange rate used in payment transactions should be implemented and calculated in a neutral manner.

Previously, the reasons for the revision of PSD1 and as a result of the adoption of PSD2 were considered in current study. Next, the anti-discrimination provisions contained in PSD2 will be analyzed. First, in the recitals, the mention of the obligation of anti-discriminatory behavior has been significantly increased in comparison with PSD1. Thus, it is noted that the Member States, as well as the competent bodies of the community, must guarantee fair competition for existing and new service providers, regardless of their business model, in order to prevent unjustified discrimination against existing market players and to ensure a stable market for services. PSD2

[85] *Supra note 83, Article 28*

stipulates that in the case of emergency situations, measures to eliminate threats must be appropriate, proportionate, and non-discriminatory, as well as properly justified.

Also, in contrast to PSD1, the recitals of PSD2 disclose the contractual provisions in more detail. Thus, they should not, by their nature, purpose, and effect, be such as are defined as discriminatory against consumers, nationality, and place of residence in the Union on legal grounds. An example is given that in the case of a change of residence of the user of payment services within the Union and if the framework agreement provides for the possibility of blocking a payment instrument for objective reasons, the paying service provider cannot invoke this right in such a case.

Regarding access to payment systems, this article provides that access criteria should be non-discriminatory and proportionate: "Member States shall ensure that the rules on the access of authorized or registered payment service providers that are legal persons to payment systems are objective, non-discriminatory and proportionate and that they do not inhibit access more than is necessary to safeguard against specific risks such as settlement risk, operational risk, and business risk and to protect the financial and operational stability of the payment system". Payment systems defined by Directive 98/26/EC remain exempt from Article 35 PSD2: "Paragraph 1 shall not apply to payment systems designated under Directive /26/EC". Also, among exceptions "payment systems composed exclusively of payment service providers belonging to a group". Moreover it is established that in case of rejection, "the participant shall provide the requesting payment service provider with full reasons". However, one of PSD2's changes to the rule under review is that the exemptions from access requirements for three-party card schemes do not apply to four-party card schemes. PSD1 envisaged a traditional four-party scheme, thus these schemes were to grant licenses to PSPs to issue cards and/or acquire transactions based on a proportionate and non-discriminatory criterion. The difference between a tripartite system that did not meet PSD1 requires that the tripartite system has discretion over which of the PSPs will be allowed to participate in any part of its scheme. This would allow three-way schemes to operate in a manner similar to four-way schemes in only some countries. In PSD2, three-party schemes have the power to decide whether any PSP can participate in any part of its scheme, however, in cases where they essentially operate as four-party card schemes, relying for example on licensees or dedicated brand partners. This clarification was provided by the Court of Justice of the European Union in Case C-643/16: "a three-party payment card scheme that has entered into a co-branding agreement with a co-branding partner does not lose the benefit of the exception provided for by that provision and, therefore, is not subject to the obligation laid down in Article 35(1) of that directive in a situation where that co-branding partner is not a payment service provider and does not provide payment services within that scheme concerning the co-branded products. However, a three-party payment

card scheme that makes use of an agent for the purposes of supplying payment services loses the benefit of that exception and, therefore, is subject to the obligation laid down in Article 35(1)." Thus, Article 35 of PSD 2 should be read in conjunction with Article 6 of the Interchange Fee Regulation, from which it can be concluded that a PSP that is authorized to purchase tripartite scheme transactions in one Member State is automatically permitted to purchase these transactions in other EU countries: "Any territorial restrictions within the Union or rules with an equivalent effect in licensing agreements or in payment card scheme rules for issuing payment cards or acquiring card-based payment transactions shall be prohibited".[86]

Additional context to the Guidance of the above article was provided by Recital 39, which states that PSPs providing services covered by PSD2 must always have payment accounts that are used exclusively for payment transactions. Consequently, the duty of Member States to provide access to such accounts was provided in a non-discriminatory, proportionate, and legitimate manner. A payment institution must provide its services in a seamless and efficient manner, even if access is basic, it must always be sufficiently broad.

The prohibition of discrimination is also mentioned in the regulations regarding access to the payment account in the case of PISP (Article 66 (4) (c) ). The action will not be characterized as discriminatory due to the presence of objective reasons, including time limits, priority, or charges to payment instructions transmitted directly by the payer. As for access for AIS access to and use of payment account information, in the absence of objective reasons, the processing of requests for account data transmitted through AISP should be non-discriminatory (Article 67 (3) (b) ).

Article 69 establishes the obligation to the PSU to use the payment instrument per the objective, non-discriminatory and proportional conditions that regulate the issuance and use of the payment instrument. And also the obligation of notifications on PIs is presented in Article 69 (1) (b): "notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorized use of the payment instrument". A common rule for both PIS and AIS is that the provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the PIS/AIS providers and the account servicing payment service providers for that purpose.

Based on objective, non-discriminatory, and proportionate criteria, as well as taking into account other legal obligations and due diligence, PSPs must decide to open payment accounts for payment institutions. For example, in the presence of triggers indicating money laundering, a credit

[86] *Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (Text with EEA relevance)*, Official Journal of the European Union 123, May 19, 2015, p. 1-15.

institution has the right to reject applications from payment institutions. AML legislation prevents the use of the financial system for money laundering and terrorist financing, which are prohibited by all Member States. Behavior inherent in AML crimes can manifest itself in the form of transfer of property if it is such that it was obtained as a result of a criminal act. Also concealing the origin of the source of the property. Transfer of rights to property, if it is known about its illegal nature under the AML. Credit and financial institutions are among those covered by the AML legislation. Illegal money flows are a threat to the integrity, stability, and reputation of the financial market. In addition, they endanger not only the development of the EU internal market but also international development. Therefore, the prevention of such activities, which should be targeted and proportionate, is necessary to eliminate money laundering and terrorist financing. The reliability, integrity, and stability of financial and credit institutions are at risk. This is the result of attempts by criminals to hide the origin of illegal income. Or directing legal or illegal activities for terrorist purposes. One of the ways of carrying out such illegal activities is the use of an integrated system of providing payment services. Hence, competent authorities are faced with the task of creating measures to preserve the stability, reliability, and integrity of the financial system. In order to achieve this goal, a balanced regulatory system of coordination measures is being created, which will allow the company to develop its business. Though, a refusal to the access account must be given to the competent authority. Such risk factors can be referred to the:

- as customer risk factors, such as unusual conduction of business relationships, cash-intensive business;
- product, service, transaction of delivery channel risk factors, for example, transactions that might favor anonymity, the absence of certain safeguards in non-face-to-face business relationships or transactions;
- geographical risk factors caused by a factor that countries are subject to sanctions identified a high level of corruption activity or/and provide support for terrorism.[87]

From the analysis carried out, it can be concluded that the principle of legality is inextricably linked with the obligation of banks not to discriminate. Banks implement their obligations to comply with the legislation on the prevention of illegal income laundering and terrorist financing, embodied in their internal policies and instructions, which are mandatory during the performance of professional activities. Thus, the presence of risk factors and the banks'

[87] *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC,* Official Journal of the European Union, 141, p. 73-117, Annex III

refusal to provide access due to them will not be considered discriminatory, as it is one that adheres to the principle of legality.

Analyzing the provisions of PSD2, it is worth noting that the criterion of proportionality goes hand in hand with the duty of non-discrimination. In the researcher's persuasive opinion, the criterion of proportionality is one of the dimensions that determine the balance of legitimate interest and means, as well as the consequences of the action, which indicate the presence or absence of discriminatory behavior on the part of banks.

In the author's opinion, there are high risks associated with payment data. Especially fraud that occurs in the event of a data breach. In order to achieve high standards of data security and customer authentication, which are key aspects of PSD2, in addition to the consolidation between different legal acts of the EU and at the same time interaction of non-discrimination, proportionality, objectivity, and legality, it is indispensable to examine reciprocal action between the PSD2 and GDPR. The purpose of the GDPR is to promote the creation of a safe, fair, and free economic union, as well as the well-being of individuals. The Treaty on the Functioning of the European Union provides that every person has the right to the protection of his personal data. Therefore, the rules for processing personal data must respect the rights and freedoms of a natural person, regardless of his citizenship and place of residence. The GDPR harmonizes such protection for processing activities and creates conditions for the free flow of personal data between Member States. The right to the protection of personal data is not absolute and therefore must cooperate with other fundamental rights and the principle of proportionality. Economic and social integration has led to an increase in the flow of personal data transfers between public and private entities. And globalization and rapid technological progress prompt the emergence of new challenges for the protection of personal data. Individuals have increasingly made personal information global and publicly available. And the development of technological progress, which has a positive impact on the development of the economy, caused the EU to ensure a high level of personal data both within the EU and during transfer to third countries. In particular, it is worth noting that the development of the digital economy requires a strong and more consistent system of personal data protection. PSD2 is not a special act concerning the GDPR but provides certain rules regarding the payment data that can be accessed. Thus, ASPSPs, PIPs, and AIPS mean that all PSPs should comply with both legal acts while providing payment services under PSD2. PSD2 sets standards to ensure that TPPs provide necessary and adequate information. The TPP providing the service is responsible for providing information to the user in the context of AIS and PIS. The legal act provides that to limit the effectiveness of providing information, it should be proportional to the needs of the user. The TPP providing the service is responsible for providing information to the user in the context of AIS and PIS.

The European Data Protection Board (EDPB) studies the interplay between GDPR and PSD2 and puts some general principles of data protection in a payment context. The obligation of service providers not to process more data than is necessary for the provision of services is emphasized. AISPs must determine the type of data required to provide services and cannot request a larger set of data from account service providers. In addition, data-sharing access is limited to paid accounts only. Service providers must ensure proper transparency, data minimization, and effective exercise of the rights of rights subjects. It is worth noting that this obligation includes mandatory informing the data subject about the presence of automated decision-making that may be applied in the implementation of FinTech.[88] Thus, the refusal of payment data providers will not be characterized as discriminatory, in the event that the requested information for TPPs is not proportionate, adequate, legal, and outside the scope of data regarding payment accounts. The researcher's opinion about the close coexistence of the obligation not to discriminate for banks with the principle of proportionality and objectivity is reflected in the analysis of the interaction of the GDPR and PSD2.

A significant breakthrough in the legal protection of individuals and groups from discrimination has not eliminated the phenomenon, which is confirmed all over the world by the fact that discriminatory acts and practices continue to take place in today's world. Discriminatory manifestations find their place in any sphere of society: education, politics, work, administration of justice, provision of social and medical services, etc, and payment services as well. Jan Krämer, Daniel Schnurr, Alexandre de Streel Project Report "Internet Platforms and Non-Discrimination" argue the reasons for the legal prohibition of discrimination at the EU and national levels, namely to improve consumer welfare and ensure fair business practices, to protect effective competition.[89] Thus, actions that lead to anti-competitive discrimination are prohibited. In this context, it is important to distinguish between external discrimination, when a firm treats equivalent third parties differently, and internal discrimination, when a firm that is vertically integrated treats its subsidiary or affiliate differently than competitors in the downstream or upstream market.

Continuing, the authors note the coexistence of non-discrimination and the obligation of transparency at the level of EU law and national regulations. The objectives of such cooperation are, for example, to reduce information asymmetry and improve the functioning of markets. The commitment to transparency is also a guarantee of EU consumer protection rules. Thus, in the specific context of the prohibition of unjustified discrimination, the obligation of transparency can help to identify violations of discrimination, which contributes to its effective application at the

[88] Niels Vandezande, *EDPB Clarifies the Interplay Between GDPR and PSD2*, February 15, 2021, Accessed September 22, 2023, URL:https://www.timelex.eu/en/blog/edpb-clarifies-interplay-between-gdpr-and-psd2

[89] Jan Krämer, Daniel Schnurr, Alexandre de Streel Project Report, Internet Platforms and Non-Discrimination, December 5, 2017, URL: https://euagenda.eu/upload/publications/untitled-121136-ea.pdf

legislative level. At the same time, the authors state that there is a justification for discrimination if it is justified if it is based on the legitimate aim it pursues, on objective and legitimate criteria, and is proportionate. The researcher agrees with the authors, especially in the part of their thesis on service, that each case must pass a test of proportionality.

Due to the growing popularity of the digital market around the world and, as a result, the large number of complaints among users about blocking due to geographical location, it is necessary to understand what geoblocking is and its legal regulation. Geoblocking is a method used by online retailers to restrict cross-border online sales by nationality, place of residence, or place of establishment. Discrimination between EU customers regarding market segmentation along national borders and increased profits to the detriment of foreign customers is considered unjustified geo-blocking. The Geo-Blocking Regulation also contains provisions declaring non-discrimination on grounds of payment. While traders remain free to accept any means of payment they wish, the Geo-Blocking Regulation contains specific provisions on non-discrimination within the range of means of payment they accept. It covers situations where the differentiated regime is the result of the customer's nationality, place of residence or place of establishment, location of the payment account, place of establishment of the payment service provider, or place of issue of the payment instrument. However, the legislator was to establish an exception, which is set out in paragraph 3 of the same article: "The prohibition set out in paragraph 1 shall not prevent a trader from charging a fee for the use of a card-based payment instrument for which exchange fees are not governed by Chapter II of Regulation (EC) 2015/751 and for which payment services not covered by Regulation (EU) № 260/2012, except where the prohibition or restriction of the right to charge a fee for the use of payment instruments in accordance with Article 62 (5) of the PSD2 is enshrined in the law of the Member State to which the merchant is subject. These fees should not exceed the direct costs borne by the trader for using the payment instrument".[90] Thus, the application of the aforementioned Directive prohibits unequal treatment of participants in payment relations.

In addition, considering the regulation of geo-blocking, first of all, it is important to find out the relation between Geo-blocking Regulation and the Services Directive. The prohibition of discrimination on grounds of nationality, which covers also indirect discrimination, is a general principle of Union law laid down in Article 18 Treaty on the Functioning of the European Union and Article 21(2) of the EU Charter of fundamental rights, as well as in the specific provisions of

[90] *Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC*, Official Journal of the European Union 60I, March 2, 2018, p. 1-15.

the above-mentioned Treaty related to internal market freedoms.[91] As far as the provision of services is concerned, that general principle is in particular specified by Article 20(2) of the Services Directive, according to which the Member States shall ensure that the general conditions of access to a service, which are made available to the public at large by the provider, do not contain discriminatory provisions relating to the nationality or place of residence of the recipient, but without precluding the possibility of providing for differences in the conditions of access where those differences are directly justified by objective criteria.[92] The possibility of application of the non-discrimination principle, as specified in this Article, relies on a case-by-case in trader's practices. Objective justification may depend, for instance, on the lack of the required intellectual property rights in a particular territory, additional costs incurred because of the distance involved or the technical characteristics of the provision of the service, or different market conditions, such as higher or lower demand influenced by seasonality, different holidays periods in the Member States and pricing by different competitors.[93] All in all, that Article remains applicable to situations not covered by the Geo-blocking Regulation. However, Geo-blocking Regulation contains the specific provisions that will prevail over Article 20(2) of the Services Directive in certain situations. The Regulation prevents traders from discriminating in the specific situations covered, without the need to carry on a case-by-case assessment of the trader's practice, and thus provides legal certainty and improves enforceability. As far as I am concerned, we have legal regulation that covers specific situations, which is at least understandable for their use both by participants in trade relations and by authorities designed to prevent and/or protect violations of rights concerning geo-blocking provide their activity. Moreover, there is a probability of inapplicability of Article 20 (2) Services Directive due to legal uncertainties and lack of enforcement actions by national authorities.

EU rules on payments require banks to: "Banks must charge the same rate for payments in euros across the EU as for an equivalent national transaction. Banks located in EU countries outside the euro area must also apply this rule and not charge more for payments in euros in another EU country than for a domestic payment in national currency. "Regarding non-discrimination, “service providers must accept any payment method, but if customers want to pay electronically

[91] European Commission, *Questions & Answers on the Geo-blocking in the context of e-commerce, 2018*, 45, URL: https://www.eccireland.ie/wp-content/uploads/QuestionsAnswersontheGeo-blockingRegulationinthecontextofe-commerce.pdf

[92] *Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market*, Official Journal of the Europe Union, 376, p. 36-38.

[93] European Commission, Commission Staff Working Document: *With a view to establishing guidance on the application of Article 20(2) of Directive 2006/123/EC on services in the internal market ('the Services Directive') Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the implementation of the Services Directive: A partnership for new growth in services 2012-2015*, June 8, 2012, URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012SC0146

(for example, by direct debit or payment card) in the currency you support, they must accept payment no matter where they or their payment service providers are. located within the EU".[94] Thus, the rights of PSU are protected in combination with PSD2 and other legal acts of the EU. PSU is free to choose the use of payment means, including with the help of TPPs. In turn, banks cannot apply differential treatment to such PSU, i.e., conduct that would be considered discriminatory, as long as such conduct does not fall under the exceptions noted above, such as operating expenses. Thus, these provisions will contribute to greater competition between new and existing participants in payment services, and this is provided for by the purpose of PSD2. The guarantee of diversity is legal regulation, which will ensure the protection of diversity in FinTech and consumer protection. And here we are faced with a dilemma that provokes a lot of debate: regulation means less innovation, but more consumer protection; and less regulation means more innovation but less consumer protection.

Traditional banks are essential to maintaining the credibility and the financial system's stability. Despite high-profile examples, they continue to have the highest level of customer confidence when it comes to financial service companies. The consequences of any imprudent behavior of the bank are catastrophic not only for clients but also for the country or even at the global level. The reputation of banks is based on security, so the level of due diligence is extremely high when banks start providing access to TPPs according to the PSD2. As in the case of any other external decision, banks in the decision to provide access to TPPs must ensure that it meets business needs, complies with the duty of care and protection of customer trust, and also does not pose a threat to risks. Insufficient regulatory regulation and an imperfect mechanism for checking the authorization of TPPs by banks lead to the emergence of obstacles in the effective cooperation of banks and TPPs. Nadja van det Veer came to the conclusion that, in line with PSD2's Article 67, the bank is not required to verify PISPs' registration and/or permissions.[95] In actuality, though, it seems sense that clients would go to the bank to sort out their issues. The author of the Thesis also concur with the author's assertion that it is possible for TPPs to misuse data at the time of deregistration (withdrawal) and later after they have disappeared.[96] The duty of care is established by assessing whether the adverse effect on the client was predictable, as frequently decided by the courts. According to common law, a duty of care is required if the bank's acts or omissions caused injury to a person. However, under the condition of unforeseeable damage, such liability will not

[94] Your Europe, *Electronic and cash payments*, June 6, 2022, Accesses, November 10, 2022, URL:https://europa.eu/youreurope/business/finance-funding/making-receiving-payments/electronic-cash-payments/index_en.htm

[95] Nadja van Der Veer, *Why gaps in the EBA Register leave worries over security*, July 19, 2019, Accessed November 10, 2022, URL:https://paymentsguru.eu/why-gaps-in-the-eba-register-leave-worries-over-security/

[96] Nadja van der Veer, *Taking a chance on TPPs: a road banks cannot afford to follow,* September 20, 2019, Accessed November 10, 2022, URL:https://paymentsguru.eu/taking-a-chance-on-tpps-a-road-banks-cannot-afford-to-follow/

arise, even if it has been established as mandatory.[97] The beginning and end of the bank's duty of care are determined differently by each legal system and court because the interpretation of the bank's duty of care varies by country and its scope depends on the legal system. Thus, they may be held liable for breach of duty of care for providing TPPs with access to their information.

As for how various legal systems handle the duty of care in banking, In the Netherlands, for instance, general banking rules have been established: "The Bank shall exercise due care when providing services. In its provision of services, the Bank shall take the Customer's interests into account to the best of its ability. None of the provisions of these General Banking Conditions or the special conditions used by the Bank shall detract from this principle".[98] As for the UK, the bank's duty of care is defined as a special and very broad concept. Instead, banks obey the principles laid out in the Financial Conduct Authority's Handbook, which consist of the requirements to conduct business skillfully, carefully, and diligently.[99] The conclusion that the duty of care is imposed on the bank in accordance with PSD2 can be made based on the following:

- Article 73: the bank is responsible for the immediate return of funds to the owner of the bank in the event of unauthorized transactions. So, in the case of PISP's fault, the bank will decode the funds of the owners of the entire bank account, and only then will they receive them from PISP. Accordingly, in case of further disappearance of the bank, it receives a financial blow;
- Article 89: the liability of banks for non-fulfillment, improper or untimely payment is established.

The EBA register does not work in real-time: "Disclaimer: The present Register has been set up by the EBA solely based on information provided by national competent authorities of the EEA Member States. Therefore, unlike national registers under PSD2, this Register has no legal significance and confers no rights in law. If an unauthorized institution is inadvertently included in the Register, its legal status is in no way altered; similarly, if an institution has inadvertently been omitted from the Register, the validity of its authorization will not be affected".[100] In addition, the essence of the EBA register is that it is only an accurate reproduction of information from national authorities: "The EBA is responsible only for the accurate reproduction of the information received by competent authorities for each natural or legal person included in the register, while responsibility for the accuracy of that information lies with the competent authorities at the

[97] Richard A Buckley, *Negligence - when does a duty of care arise?*, Accessed November 11, 2022, URL:https://www.lexisnexis.co.uk/legal/guidance/negligence-when-does-a-duty-of-care-arise

[98] Wagennar Lawyer, *Duty of Care Banks*, January 2, 2017, Accessed November 11, 2022, URL:https://www.wagenaarlawyers.nl/en/termination-credit-agreement/

[99] Financial Conduct Authority. *Principles for Business. Chapter 2. The Principles*, January 3, 2018, URL:https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html

[100] European Banking Authority, Payment Institutions Register, Accesses November 15, 2022, URL:https://euclid.eba.europa.eu/register/pir/disclaimer?returnUrl=%2Fpir%2Fsearch

national level".[101] Therefore, banks' reliance on public registers is insufficient. In addition, information from national competent authorities is also lacking. So, for example, the format in which the information is presented, such as PDF (register of Liechtenstein and Ireland), is not machine-readable. Even a brief examination of the authorization status is insufficient. For example, Ipagoo's (the British FinTech company) status was suspended, but the FCA header's authorized status was kept. Below the records, a remark has been put stating that the firm has been suspended from all activities.[102] Taking into account the reviewed information, the author of the Thesis conclude the need for technical improvement of the interface of such registers that will meet the requirements of today's rapidity. Therefore, the relevant authorities should pay special attention to the elimination of such inconsistencies to ensure the smooth provision of payment services.

Electronic IDentification, Authentication and trust Services (eIDAS) certificates do not solve problems either. The eIDAS certification establishes the requirements and standards for online trust services, qualified certifications, qualified electronic signatures, qualified advanced electronic signatures, and simple electronic signatures. It also governs the administration of electronic transactions. The face-to-face presence act required before getting a certificate at a Registration Entity is avoided thanks to the eIDAS Regulation, and its achievement is permitted through a distant digital channel, as it is stated in Article 24.[103] The eIDAS framework controls the certification of a certified electronic signature, making it feasible to maintain trust in a person's identity when using a certificate from another trusted source. By doing this, a new environment for electronic administration is developed, and adding new users only requires one click. According to PSD2, banks are obliged to rely on eIDAS certificates when establishing a communication channel for identification and authentication. This covers the functioning of the Qualified Trust Service Providers (QTSP) that issue them as well as standards created to confirm the identification of their holders. As "Qualified Certificates," eIDAS Certificates that are issued in line with eIDAS standards by QTSPs have a unique standing in several legal and regulatory contexts within the EU.[104] EIDAS Certificates only confirm the regulatory status at the time of issue. However, in case of revocation of the TPPs permit by the national regulator, such information is not reflected in the eIDAS certificate. This is due to the fact that cooperation between the parties issuing IDAS certificates, namely the national regulator and the relevant

[101] *Supra note, 89*
[102] *Supra note 83*
[103] *Regulation (EU) No 910/2014 of the European Parliament and Council of July 23, 2014 on electronic identification and trust services for electronic transaction in the internal market and repeating Directive 1999/93/EC*, Official Journal of the European Union, 257, August 28, 2014, p. 73-114.
[104] Electronic IDentification, *eIDAS: The Digital Identification Regulation for Europe*, May 12, 2022, Accessed November 18, 2022, URL:https://www.electronicid.eu/en/blog/post/eidas-regulation-electronic-signature/en

QTSP, has not been established at the legislative level. The EBA only indicated a voluntary cooperation mechanism for the suspension of an authorization, not its withdrawal.

The question of balancing the duty of care placed on banks and the barriers to access for authorized TPPs due to such a duty is acute. In order for banks to have complete and up-to-date information about TPPs, they need to create continuous real-time status checks. Thus, any decisions of regulatory bodies regarding TPPs should be promptly made known to banks. In this way, banks will be able to protect themselves and their customers exposed to risk and unscrupulous and incompetent TPPs. Some banks use private registries to identify TPPs in real-time and check regulatory statuses, such as the Open Banking Directory and PSD2 API Tracker. Some of these providers further reduce banks' liability for risk by providing insurance services on the information they provide. However, banks still have an obligation to check all possible risks when making such an external decision to protect their customers.

To sum up, carrying out the analysis allows us to conclude that there are more non-discriminatory provisions and aspects subject to introducing non-discriminatory behavior in PSD2 than in PSD1. PSD2 requires banks to provide access to their customer's data in a non-discriminatory, proportionate, and objective manner to develop a competitive integrated internal market. The non-discriminatory nature of the behavior is also mandatory for changing the contractual provisions, calculating the payment service rate, and solving emergency situations. Since EU law is characterized by the consolidation of legal acts and the coexistence of legal principles, the obligation of non-discriminatory behavior is accompanied by the principles of legality, proportionality, and objectivity, it is worth consider non-discrimination obligations in the interaction with other legal acts such as AML Directive, GDPR, Geo-blocking regulation, and Service Directive.

### 2.3 Summary

The analysis of the legal nature of FinTech and its practical significance leads to the conclusion that FinTech is not a completely new phenomenon and demonstrates its successful usage all over the world throughout timelines. In addition, taking into account the development and application of innovative technologies in the payment sector, "traditional banks", wishing to remain competitive, provide the best service, and maintain the loyalty of their customers, are intensifying cooperation with FinTech for this purpose

Recent theoretical developments have revealed the absence of a legal definition of FinTech mainly due to which new and innovative technologies result in the creation of new and innovative business models and products is unclear. In addition, there is a view of the rapid loss

of legal definition if adopted, given the current rapid pace of technology development, which, unfortunately, is not a solution to conflicts related to the application of FinTech, and therefore, the position previously expressed on the need for legal certainty of FinTech remains a matter of debate.

Due to its attributes such as security, speed, immutability, innovation, value, and trust, FinTech is an acceptable and promising method of data interchange, particularly in the B2B sector. FinTech also encourages effective competition in the single EU internal market, which is consistent with the strategic orientations of its growth.

Carrying out the analysis allows us to conclude that there are more non-discriminatory provisions and aspects subject to introducing non-discriminatory behavior in PSD2 than in PSD1. Since PSD2 aims to develop a competitive integrated internal market, PSD2 requires banks to provide access to their customer's data in a non-discriminatory, proportionate, and objective manner. Moreover, the non-discriminatory provisions of the PSD refer to the calculation of the payment service rate, so it should be calculated neutrally. In addition, PSD2 declares the resolution of emergency situations in a proportionate, legal, and non-discriminatory manner. The non-discriminatory nature of the behavior is also mandatory for changing the contractual provisions. Since EU law is characterized by the consolidation of legal acts and the coexistence of legal principles, the obligation of non-discriminatory behavior is accompanied by the principles of legality, proportionality, and objectivity. Thus, such behavior will not be considered discriminatory, for example, if it is justified to prevent a violation of money laundering legislation. In addition, the amount of information to which TPPs can be given access is determined by the GDPR, which also excludes the discriminatory behavior of banks toward TPPs. The prohibition of discriminatory behavior is also dictated by the Geo-blocking Regulation and Services Directive. Finally, the cautious behavior of banks in cooperation with TPPs, which may seem restrictive at first glance, is actually due to their duty of care.

## 3. FINTECH AS A THIRD-PARTY PLAYER

### 3.1 Access to the Payment Information for Third-Party Providers

The debate over whether the laws governing this technology should come first, or the technology itself, is merely philosophical. Without a thorough understanding of how technology regulation actually functions in practice, it is impossible to forecast all scenarios and features of it. On the other hand, effective governmental regulation that safeguards the rights of interested parties is necessary for the existence and implementation of technology. PSD2 was the result of the revision of PSD1 and for the reasons that the constant development of the technological process caused the emergence of new interests of consumers and providers of payment services that require appropriate protection. PSD2 came into force in 2018, and since then, with the development of new technologies, as well as the fact that the studied Directive is consolidated with other legal acts of the Union, new challenges have arisen for all participants in the provision of payment services. Therefore, the author agrees with the scientists and the conclusions of the competent authorities about the need to revise PSD2. The necessity or its absence of revising the provisions of PSD2 will be analyzed below precisely from the point of view of proper and sufficient, in other words, effective declaration of non-discriminatory provisions.

The precursors of open banking were preceded by aggregation sites such as Mint or Personal Capital. They combine the client's financial information from all financial institutions, with the aim of locating them in one place. The aforementioned platforms require the customer to submit their user credentials and passwords from each customer account, and then capture data from the screens of the provided accounts. However, this method is risky for security. In addition, the result of the screen scan is not always accurate. In addition, not all financial institutions are compatible with such platforms, which prevents a complete impression of finances. The API used for Open Banking is more secure because applications exchange data directly without providing account credentials.[105] Therefore, it is open banking that meets the technical conditions that determine the security of providing payment services.

Previously, only banks, central banks, or government institutions could provide payment services. PSD1 introduced a new category of participants in payment relations - PSP. In addition, PSD1 became a regulatory framework that allowed new non-banking organizations to provide payment services. Thus, banks have become transparent about their services and fees, exchange rates, and payment processing times. The implementation of PSD1 accelerated the development

[105] Congressional Research Service, *Open Banking, Data Sharing, and the CFPB's 1033 Rulemaking*, September 9, 2021, URL:https://crsreports.congress.gov/product/pdf/IN/IN11745

of SEPA, which represents a single payment area in euros to facilitate payments. Thus, European clients, regardless of the form of ownership, gained access to faster and cheaper services in the EU and EEA. PSD1 also had a positive impact on the development of FinTech, which combined the possibility of providing access to new services, lower prices, and a better experience.

Thus, access to the payment system was established by PSD1. Article 28 stipulates that PIs authorized in other member states have the same right of access and non-discrimination as PIs authorized in the Member State where the payment system is based. In turn, PIs have the right to set their access criteria to their systems only under the condition of their objectivity, non-discrimination, and proportionality. This article was adopted with the aim of strengthening competition in payment markets, ensuring equal conditions for all its participants, by removing barriers to the emergence of new participants (non-banks). A payment institution/non-bank wishing to create a new payment card system and gain access to the market has the right to access the Online To Bank (OLTB) payment authorization infrastructure on non-discriminatory and proportionate terms. The OLTB system allows access to deposits on the client's bank account, provided that such consent has been previously authorized by the client. Without providing access to such a system, a new payment institution cannot exist and, accordingly, the goal of PSD1 to increase competition between different payment systems is not achieved. Therefore, Article 28 guarantees access to technical components of banking systems on objective, non-discriminatory and proportional terms, which can be presented in the authorization network created by banks. Article 28 stipulates that PIs authorized in other member states have the same right of access and non-discrimination as PIs authorized in the Member State where the payment system is based. In turn, PIs have the right to set their access criteria to their systems only under the condition of their objectivity, non-discrimination, and proportionality.

This article was adopted to strengthen competition in payment markets and ensure equal conditions for all its participants, by removing barriers to the emergence of new participants (non-banks). A payment institution/non-bank wishing to create a new payment card system and gain access to the market has the right to access the OLTB payment authorization infrastructure on non-discriminatory and proportionate terms. The OLTB system allows access to deposits on the client's bank account, provided that such consent has been previously authorized by the client. Without providing access to such a system, a new payment institution cannot exist and, accordingly, the goal of PSD1 to increase competition between different payment systems is not achieved. Therefore, Article 28 guarantees access to technical components of banking systems on objective, non-discriminatory and proportional terms, which can be presented in the authorization network created by banks.

To begin with the consideration of the application of FinTech, PSD2 is the main driver among EU legislation for open banking. Open banking is a "banking practice that provides third-party financial service providers open access to consumer banking, transaction, and other financial data from banks and non-bank financial institutions through the use of APIs".[106] The author of the Thesis agrees that Open Banking is a hub of financial innovation that is undeniably impacting and changing the banking industry. Between 2020 and 2024, the global open banking user base is anticipated to increase at an average annual pace of about 50%, with the European market being the largest. Around 12.2 million people in Europe used open banking in 2020. By 2024, it is anticipated to reach 63.8 million. Open banking services were utilized by 24.7 million people as of 2020; by 2024, that figure is expected to rise to 132.2 million.[107]

Open banking allows you to combine accounts and exchange data between institutions for use by consumers, and between financial institutions and TPPs. Abandoning centralization in favor of using a network helps payment service clients securely share payment information with other financial institutions. For example, open banking eases the difficult process of transitioning from one bank's checking account service to another bank's service. A recent shift in people's perceptions and expectations brought on by Internet services other than banking is what gave rise to open banking and the requirement for such a model. People expect the same kind of experience and appeal from banking services and have the power to choose what they will use and in which channel because they are accustomed to interoperable experiences like those offered by social networks or smooth like those provided by e-commerce sites, for instance.

The advantages of open banking are:

- helps clients get a more accurate picture of their finances;
- helps determine the best financial products and services for the client, thanks to the received information on its transactions;
- helps small businesses to simplify their management thanks to online accounting;
- helps fraud detection companies more effectively monitor customer accounts and detect problems more effectively;
- helps lenders get an idea of the client's financial condition and level of risk in order to offer more favorable loan terms in the future.

In the author's opinion, open banking is an impetus for positive changes both for large, well-known traditional banks and for new participants in payment services. Open banking provides

[106] Open Bank Project, *Open Banking API Platform. What is the Open Bank Project Platform?*, Accessed November 18, 2022, URL:https://www.openbankproject.com/openbankingmiddleware/

[107] Statista Research Department, *Open banking users worldwide in 2020 with forecasts to 2024, by region*, 31 May, 2022. Accesses November 18, 2022, URL:https://www.statista.com/statistics/1228771/open-banking-users-worldwide/

access to the market of payment services for new participants, thereby creating a competitive environment. Because of this, traditional banks are forced to reduce costs and adopt new technologies to provide a better customer experience. In turn, this will lead to the need to review the business of traditional banks, introduce their new policies and spend money on new technologies. However, it will allow banks to improve customer relations and retain them.

At the same time, the disadvantages of open banking include:

- the growth of the FinTech market, which offers various payment services in a simpler, faster, and cheaper way for customers. FinTech can provide many services that "traditional banks" provide and thus reduce their popularity;
- open banking is a relatively new concept, and many mistakes still happen;
- relative mistrust on the part of clients, which is associated with the fear of transferring personal and payment data, which is caused by insufficient knowledge of the principles of open banking;
- digitalization reduces personal contact with the client, which leads to a decrease in loyalty to the company's brand between the client and the supplier;
- open banking APIs are not completely free from security threats, hacker attacks, etc. And combining data can only create a favorable environment for criminals.

However, from a researcher's point of view, the advantages of using open banking outweigh the disadvantages. After all, the loss of popularity of traditional banks and the decrease in the loyalty of their customers depends on the conduct of the business of such companies, which must be able to quickly adapt to modern conditions. Also regarding security risks, FinTech companies pay great attention to this aspect and implement all possible tools that will prevent security breaches and hacker attacks. In addition, FinTech companies think and develop in advance scenarios from the algorithm of actions, in case such a security breach occurs, with the aim of promptly solving it and effectively entrusting the protection of the violated rights of users.

The Investopedia team also expresses concern that increased competition between TPPs and traditional banks could lead to the consolidation of financial services.[108] This will backfire on consumers and will not lead to the expected reduction in customer spending. However, the author of the Thesis believes that since consumer capacity does not increase due to negative global processes, due to the crisis and increased inflation, consumers will not agree to pay more. In such a scenario, the creation of new technologies and methods of providing payment services is more likely.

[108] The investopedia Team, *Open banking: Definition, How it Works, and Risks*, April 4, 2022, Accessed November 19, 2022, URL: https://www.investopedia.com/terms/o/open-banking.asp

As it was mentioned before, open banking allows TPPs to get access to the payment transaction and other data from banks and other PSPs due to APIs. API is an interface of application programming which is inherently a technology that enables a network of different IT systems that can share information that in turn should conform to the specification of standards set out by Open Banking Standard. The API makes it easy to manage payments for e-commerce businesses. APIs make transactions fast and secure, so they make the payment process more efficient for both PIs and consumers. Regarding the cost of using APIs, some of them are free, depending on the provider. And some may charge a fee for processing the payment, depending on the payment instrument used. Because APIs can act as credit card processors, they can accept credit or debit card payments, as well as bank account payments. Thus, companies can offer the most convenient payment method for their customers. Companies also use the API to report tracking payment information. So, as for the benefits of APIs, they automate the payment process, and thus, less time and resources are required for merchants to maintain such systems, which is quite a good business decision. In addition, the API can be configured and scaled conveniently, as well as integrated with other electronic tools and programs.[109] Moreover, API helps to integrate local and global payment options such as digital wallet payments, bank transfers, etc. Also, it is possible to track orders and access real-time payment data per transaction. Additional criteria when choosing an API is compliance with security standards.[110] And last but not the least API makes it easier to accept and reach customers in international markets. When choosing an API, pay attention to:

- features - analysis of API functions allows us to determine its compatibility with the current business model of the enterprise;
- price poisoning - it should be emphasized that it should be transparent and understandable for users and providers of payment services;
- ease of use and integration - the interface should provide effective interaction between the user and the client.

Following PSD2, banks are required to offer APIs in certain, limited contexts; in addition, other financial institutions involved have chosen to make the API available on Gold's behalf. Several financial institutions are functioning in European environments, hence standardization efforts have started to emerge. The crucial ones are:

[109] Sara Heegaard, *What is a payment API?*, August 31, 2021, Accesses November 19, 2022, URL:https://rechargepayments.com/glossary/payment-api/

[110] Stax, *Payment APIs: What Are They and How do They Work?* Accessed November 19, 2022, URL:https://staxpayments.com/blog/payment-apis-how-they-work/

- PolishAPI: The Association of Polish Banks is developing the PolishAPI standard in conjunction with commercial banks, related cooperatives, and TPPs. This standard specifies a user interface for TPPs that require access to payment accounts.
- Slovak Banking API: The Association of Slovak Banks is working on this standardization project with the Slovak National Bank, and documentation for it is available;
- The STET standard, a French clearinghouse effort;
- NEXTGenPSD2: From a pan-European viewpoint, the Berlin group is in charge of this standardization endeavor.[111]

Discussions about PSD2 open banking compliance are being held by competent EU entities. For instance, Euro Retail Payment Board (ERPB) is a strategic advisory group at the ECB. This organization released two reports in May 2019 and June 2021 outlining a program known as the "SEPA API Access Scheme." The following subjects are covered by the ERPB proposal and will be discussed with the General Directorates of the European Commission[112]:

- specifying techniques and standards for implementing the chosen services based on the usage of APIs, as well as the guiding principles for collaboration between the parties involved;
- a system for billing and paying for services that takes advantage of APIs;
- the way that potential services are monetized;
- the PSD2-related services offered by European financial institutions to third parties would continue to be free;
- other service kinds (extended, value-added, premium, and so forth), per country-specific legislation, may be monetized by credit institutions.

TPPs are presented by 2 groups of such providers: AISP and PISP which mainly can be distinguished by the possibility of initiating activity from the account, for example, such as payments. To begin with, AISP may provide account information services by collecting only the reading of financial information. AISPs are able to gather data from various bank accounts with the explicit consent of PSU but they do not have the competence of initiating activity. PSD2 designates PSU as “a natural or legal person making use of a payment service in the capacity of the payer, payee, or both”.[113] Thus they are not able to make any payments from those accounts. In addition to the obligation to provide services only with the consent of the PSU. PSD2 inserts other rules for AISP. In particular, AISPs must ensure that PSU data will not be available to other

[111] Mario Palmieri, *Open Banking PSD2 regulation in EU*, July 14, 2022, Accessed November 21, 2022, URL:https://FinTechlegal.center/open-banking-psd2-regulation-in-the-eu/
[112] Euro Retail Payments Board, Report Next Phase of the ERPB WG on a SEPA API Access Scheme, June 28, 2021, 111, URL:https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/15th-ERPB-meeting/Report_from_the_ERPB_working_group_on_a_SEPA_API_Access_Scheme.pdf?52770756a713895bdc4fd072873346be
[113] *Supra note 3, Article 4 (10)*

parties and that their transmission goes through secure and efficient APIs. AISPs shall only have access to information from designated payment accounts and related payment transactions and shall not use, store, or have access to any other data for any other purpose.[114] AISPs rely on other regulated companies known as Account Servicing Payment Service Providers (ASPSPs). Banks, PI, and credit providers are among ASPSPs.

I will consider the stage-by-stage work of AISP, the participation of PSU, their interaction with PI, as well as the rights and obligations of participants dictated by PSD2. First of all, PSU chooses ASPSP where the account is held. The PSU must identify the ASPSP to the AISP so that the request creates access to the data capabilities of the ASPSP, which must be available to all TPPs. The AISP is tasked with providing sufficient information for the PSU to make an informed decision, i.e., the purpose for which the data is used, the period of information request and the moment of termination of consent to the account information must be specified in detail, as well as whether other parties will have access to such information. AISPs are required to indicate the commercial name of the company or brand for the PSU when processing the consent request. The PSU is obliged to confirm its consent to AISP for the use of services every 90 days. The AISP must confirm to the PSU that the account information request has been successfully completed. To continue with, PSU is directed to the domain of its ASPSP for authentication to choose the account to which access should be given. As soon as authentication is done, ASPSP will respond to the request from AISP and provide the requested data. Taking into account the rules established by the PSD2, the AISP acts on behalf of the PSU. Thus, the PSU can use AISP services only within the parameters of the user's delegated rights.

AISPs gained popularity as a money management tool among their users. Among other advantages of using AISPs is that companies that get access to bank account data get reliable information about the financial capacity of their customers. AISP users also have the possibility of smart budget planning through personal finance applications. One of these is Plum, which researches the purchases of its users and provides personalized savings recommendations thanks to opportunities to limit spending. In addition, thanks to AISPs, there is an opportunity to speed up the assessment for creditors. Zopa - a British company that provides financial services for deposit accounts and credit cards, calculates the affordability of repaying loans using user data on income and expenses. Compared to other potential competitors, the company can make faster decisions on service approvals and reduce administrative costs. Another advantage of AISPs is the ability to increase the satisfaction level of the customer experience thanks to better visibility of financial data and ease of use. For example, Revolut uses AIS to create a technology that

[114] *Ibid, Article 67*

aggregates all accounts into one.[115] Thus, in author's of the Thesis opinion, the advantages of AISPs are provided both for PSUs and for PI.

As for PISP, they provide payment initiation services. Therefore, unlike AISPs, they can transfer money from the client account, as provided for in PSD2, only with the consent of the PSU. The GDPR's (explicit) consent is distinct from the PSD2's explicit consent. An additional criterion of a contractual character is the explicit consent required under PSD2 Article 94(2). The PSU must expressly consent per Article 94(2) of the PSD2 whenever a PSP needs access to personal data to perform a payment service. In other words, PISP executes a transaction on behalf of the client. In the same way as for AISPs, for PISPs the rules of PSD2 regarding the implementation of payment services are established regarding the mandatory consent of the PSU to guarantee the security of information and its provision only through secure channels to the extent determined by the necessity of the transaction. Taking into account the specifics of PISPs, namely the possibility of transferring money, an additional obligation of PISPs is the prohibition of changing the amount, the payee, and their transfer characteristics; the prohibition to withhold the payer's funds at any time for the purpose of providing PIS. In addition, payment orders that were transferred through PISPs ASPSP should be considered in a non-discriminatory manner, in the absence of objective reasons regarding time, priority, or charges regarding payment orders transferred directly by the payer.

As for how the payment service is practically carried out with the participation of PISPs within PSD2, the researcher would like to consider an example of when a customer needs to pay for a product or service online. The client encourages the transaction by choosing the goods or service that needs, which can be completed in a variety of methods, like by scanning a QR code or going to an online payment website. Customers are offered the choice to pay with their bank account when prompted. Only if the customer chooses the "pay by bank method" will PISPs start these account services. This payment method makes use of a banking API, which makes data exchange simple and secure. To deduct money from the customer's bank account, the PISP uses the banking API.

As for the advantages of using PISPs, according to the researcher's opinion, both clients and beneficiaries of payment services benefit. On the part of customers, this allows for a better customer experience, because open bank payments are less complicated for customers to make because customers enter less data and have to perform fewer actions than other methods require. For merchants, open bank payments also help reduce their costs due to lower operational costs for payment processing, and instant settlement allows for faster transactions and less complex cash

[115] Matthew Blenkarn, *What does AISP & PISP mean?*, March 9, 2022, Accessed November 20, 2022, URL:https://truelayer.com/blog/what-does-aisp-pisp-mean/

flow. Moreover, PISP can also be an example of a successful financial management tool, for example by transferring money to a personal saving account. As for business solutions, PISPs can be used as a back office for greater payment visibility. The delivery application is a more routine example. It is also possible for the app itself to initiate a payment transaction on behalf of the customer in the amount of the order rather than requiring the customer to enter their credit card information. According to this instruction, the restaurant will receive the money from the bank holding the delivery app customer's account.

There are several advantages to using PISP, but the most important is the aspect of security. Due to the fact that PISPs employ Strong Customer Authentication (SCA), payment fraud is greatly reduced, as bank transfers are only initiated after payers authenticate the transaction using SCA, which greatly reduces payment fraud. SCA is characterized by PSD2 as authentication that relies on the utilization of two or more elements. The first of them is referred to as knowledge or information that only the user is aware of. The user-specific ownership comes next. Affiliation, or who the user is, is another factor. These components are made to safeguard the confidentiality of the authentication data and are separate in that a breach in one does not affect the dependability of the others.[116] Member States must make sure a PSP uses SCA whenever an account holder: (a) gains access to its payment account online, (b) enacts an electronic payment, or (c) performs any other action through a remote channel that could potentially involve a risk of payment fraud or other violations.[117] In practice, the application of SCA looks as follows. Firstly, a cardholder desires to make a purchase, so they enter in their name, card number, CVV, and expiration date. Then a new popup from the bank appears and requests any of the following:

- something they know, for example, a PIN which is already set;
- something they have, such as their phone, which they verify by entering a One Time Password they got through SMS;
- something they are, like a scan of their fingerprint or a photo of their face.

As a result, the payment is approved if the information matches what is on file.[118]

SCA actively tries to reduce the use of credit card fraud, including the use of card information obtained illegally through the use of card cloning or testing by criminals. Additionally, SCA eliminates some cases of chargeback fraud by verifying the customer's identity as the cardholder. Therefore, card-related crimes may be committed by fraudsters far less frequently, while banks, merchants, payment processors, and customers are all better protected. Accordingly, the author comes to the following conclusion: it follows that PISPs will be denied access to the

[116] *Supra note 3, Recital 30*
[117] *Supra note 3, Article 97*
[118] SEON, *What is Strong Customer Authentication (SCA)?*, Accessed November 20, 2022, URL:https://seon.io/resources/dictionary/sca/

account if SCA is failed, making it impossible for them to complete the transaction. Therefore, a rejection of this form cannot be viewed as discriminatory because it is justifiable for security concerns.

Similarly, with the PISP approach, customers only submit their credentials once with their bank and never provide them to the merchant or payment gateway. This lessens the risk for consumers (possible fraud in the future) and businesses (from data breaches), fostering customer and potential customer confidence that their information is secure when they make transactions.

ASPSPs may discriminate against TPP-initiated transactions or information requests only for objectively justified and properly substantiated reasons related to unauthorized or fraudulent access to the payment account and must allow access again when the reasons for denying access no longer exist. If an ASPSP denies access to a TPP, it must also notify the PSU and its national regulator. Therefore, ASPSPs should consider the parameters they will use when deciding whether to reject or delay TPP-initiated transactions or requests for information.[119]

Thus, for the technology of open banking, as for any bank transfer, cheap payment service and speed of the transfer remained beneficiary for merchants. However, the indisputable advantage provided by the development of FinTech and the availability of legislation in the form of PSD2 were:

- speed and ease, because consumers do not need to leave the web page to make a payment. The exchange of payments takes place automatically in a safe way thanks to APIs, and authentication with the bank takes place thanks to automatic redirection;
- security: the correctness of the recipient's data is no longer the responsibility of the consumer. Instead, thanks to open banking, all data exchange takes place, preventing misdirected payments and fraud.[120]

The focus of researcher's attention is on the obstacles that TPPs still face when entering the payment services market. First of all, these are differences in interpretation caused by the implementation of the PSD2 into national legislation. For example, the PSD2 assumes that TPPs have access to "payment accounts" that other payment service providers have. According to the PSD2, a payment account is an account used to execute payment transactions[121]. Ordinary bank accounts where a user can deposit, withdraw and execute transactions are thus considered payment accounts. In the case of mortgage accounts that do not fall under this definition, they go beyond

[119] Clinford Chance, *PSD2 implementation: What you need to know,* September 2017, p.7 https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2017/09/psd2-implementation-what-you-need-to-know.pdf

[120] Jack Wilson, PSD2 4 years on: why open banking is a success - and how to judge it, January 13, 2022, Accessed November 20, 2022, URL:https://truelayer.com/blog/psdon2-4-years-on-why-open-banking-is-a-success-and-how-to-judge-it/

[121] *Supra note 3, Article 4(12)*

the PSD2. Another example of legal uncertainty and the consequence of the different application of the PSD2 rules due to implementation in national law is the use of credit cards, as most credit card accounts are probably not covered by a "payment account" as users cannot deposit funds into these accounts. On the other hand, users are allowed to withdraw money from the account and make payment transactions. Thus, TPPs that provide services in several EEA countries may have access to credit card account data in one country, while banks in another country do not provide this data. The main conclusion that can be drawn is the creation of effective competition in the provision of payment services and the improvement of the general condition of the banking sector, as well as the improvement of consumer protection and the successful introduction of new payment technologies. However, TPPs such as FinTech, e-commerce, and other start-ups still face regulatory barriers to entering the payments market due to the ambiguous implementation of PSD2 provisions into national law and, consequently, the lack of a unified approach to regulating the same aspects in different EU countries.

Having analyzed the categories of TPPs and researched specific examples of world-famous FinTechs, for me the fundamental reason for their success is the implementation of payment services per the rules established by PSD2, in particular concerning the non-discriminatory aspect. After all, the Directive provides the possibility of data access for AISPs and PISPs, however, at the same time, such access can be carried out only with the client's consent and can be limited by financial institutions in the amount of providing such data or rejecting such access only in the presence of objective reasons established EU legislation.

### 3.2 The Current Role of FinTech and its Future Perspective

In August 2016, the UK's Competition and Markets Authority (commonly referred to as the CMA) issued an order requiring the country's nine largest banks — Barclays, Danske Bank, Santander, Lloyds, Bank of Ireland, HBSC, RBS, Allied Irish Bank and Nationwide — to give authorized businesses or startups direct access to their data, particularly to transaction-account transactions. The CMA directive became effective in January 2018. It made use of protocols and tools developed by Open Banking Limited, a nonprofit established with this objective in mind. This legislation operates per the general Open Banking PSD2 requirements that apply to all providers of payment account services and is only applicable to the nine banks previously specified. The Competition and Markets Authority is in charge of enforcing the directive; the Information Commissioner's Office and the FCA are in charge of protecting consumers' privacy regarding data and information related to account and payment order activities in the UK. There are 202 FCA-regulated providers who have signed up for Open Banking as of January 2020. Many

of them offer financial services applications (such as those for managing finances), but there are also consumer credit firms that use Open Banking capabilities to access data on bank accounts for accessibility and check reasons.[122]

In the author's opinion, it will be appropriate to speed up the practical application of FinTech, namely AISPs and PISPs per PSD2 on the example of another financial institution, to which the researcher has a direct relationship as an employee of its group. Thus, Danske Bank is the largest commercial bank in Denmark and one of the leading banks in Northern Europe. By providing TPPs with direct access to banking information, Danske Bank opens up huge opportunities for the consumption of new services for its customers, as well as new business opportunities for companies. The development of open banking increases the level of customer experience by assisting them in managing the finances of its customers easily. As for open banking in practice, Danske Bank presents some successful illustrations of utilizing open banking. One of them is MobilePay which is used by customers for fast and effective transfers and is currently the most popular payment solution in Denmark. One more example of open banking that has a relationship to the Danske Bank is Aiia. Aiia is licensed for both AISP and PISP and by one single API to all Nordic banks. Thus, its usage is possible for business as well as for personal money management for creating financial services. Furthermore, Danske Bank has a partnership with Swedish FinTech Minna Technologies. Minna Technologies is a service provider for managing personal finance by managing subscriptions in their apps. Complying with provisions of PSD2, Danske Bank clients are not automatically included single API connected to all Nordic banks. m open banking services, only with permission provided by clients' consent every time during usage of payment services where regulated TPPs are involved. Danske Bank states that clients control access to their data, which TPPs they want to use, the scope of access to the information that can be used as well as the period for such usage. Danske Bank assured their client the safety of open banking by using only strictly tested software and secure systems is a priority. Moreover, all TPPs solutions have to be regulated to use Danke Bank's secure infrastructure.[123] In researcher's opinion, such a partnership of a "traditional bank" with other FinTechs determines its success in the market of payment services and loyalty among its customers. It is the provision of effective access for TPPs that allows you to be on time and increase your competitiveness.

Returning to the statement that was made at the beginning of this section that there is no clear answer to what should precede law or technology, for researcher it was found out the answer that the most optimal solution lies in the prompt adoption and/or change of the current legislation.

[122] *Supra note* 111
[123] Danske Bank, *What is open banking?* Accessed November 10, 2022, URL:https://danskebank.com/about-us/openbanking

Therefore, for payment services, updating the legislation, namely PSD2 with the aim of relevance and effective implementation with the participation of FinTech, is an inevitable process, which is already being actively discussed among specialists and competent authorities. In particular, the part of providing effective unimpeded access, i.e. non-discrimination on banks.

In the long term, the non-discriminatory behavior of banks concerning TPPs will contribute to strengthening their position in the market. So, in addition to selling its products and services, the bank can facilitate TPPs to sell their products and services through their institution. Thus, banks will have a greater influence on the form and manner in which these products or services will be provided to their customers. At the same time, the bank will have leverage in determining the value of such a partnership. Due to constant technological changes, it can be concluded about the fundamental importance of such a partnership for "traditional financial institutions", which will also be affected by regulatory and commercial conditions of coexistence.

The feeling that it is not necessary to evaluate and revise PSD2 for the purpose of effectiveness and compliance with modern conditions, introduced the emergence of discussions and consultations of the competent EU bodies and specialists in payment services. For example, Kimberly Moran identified the main problems faced by TPPs under the current conditions of established PSD2, in particular:[124]

- poor API quality makes it impossible to gain access to consumer accounts. Thus, PSUs are redirected back to the ASPSP for authentication and must manually enter account information themselves, as a result of which access is also denied;
- problems with SCA. PSUs must re-authorize the use of TPPs every 90 days for AIS. As for the PISP, the PSU can be offered up to 4 times the SCA for a general transfer. Currently, starting in March 2022, the FCA strongly recommends that banks apply an exception where authentication is required only the first time a customer provides access to their AISP data;[125]
- uneven adoption and implementation of PSD2 provisions by Member States. This leads to the appearance of inconsistencies and discrimination of International Bank Account Number (IBAN) against non-local numbers;
- daily limits on API calls, which lead to loads on TPPs.

According to the author of the Thesis, the problem should not arise so acutely, because as the researcher has previously discussed in this section, when choosing an API, it is necessary to pay attention to the characteristics of the API, in particular its functions, to identify its compatibility with the current business model of the enterprise. In addition, a criterion was

[124] Kimberley Moran, *PSD2 in review*, July 5, 2022, Accessed February 6, 2023, URL:https://plaid.com/blog/psd2-in-review/

[125] Jack Wilson, *Explaining changes to the 90 day rule for open banking access*, February 14, 2022, Accessed February 6, 2023, URL:https://truelayer.com/blog/explaining-changes-to-the-90-day-rule-for-open-banking-access/

established for the ease of use of the API and its integration. Moreover, as noted in the report of The Euro Retail Payments Board (ERPB) analyzed above and the recommendations from it, the specification of techniques and standards for the implementation of selected services based on APIs, as well as the principles of collaboration between all participants of payment services, are the subject of discussion among the competent authorities.

As for the necessity of reviewing PSD2, one of the discussed aspects is open finance, which is a kind of extension of open banking. Under PSD2, TPPs only have access to defined customer data, but an initiative is being discussed to expand access rights to additional customer data, such as mortgages, savings, pensions, and insurance services. Thus, open finance will expand the list of financial and information services. In the author's point of view, such a change is appropriate, because the effectiveness of cooperation between TPPs will clearly be increased, which will increase satisfaction among customers of both TPPs and traditional banking.

Taking into account the prospect of the expansion of direct banking to open finance which will be supported by various TPPs, it will be appropriate to consider the prospects of FinTech with the use of AI. Aaron Klein of the Brookings Institution states, that "America's current legal and regulatory structure to protect against discrimination and enforce fair lending is not well equipped to handle AI".[126] We agree with the author that "discrimination and bias are significant issues in a data-dependent financial technology system."[127] At first glance, the decisions made due to the use of technology are objective. However, the author's assumption about the "error of neutrality" is relevant. It manifests itself in the fact that artificial intelligence-driven technologies can use seemingly neutral data to "assess the potential of marital problems through support measures that study travel, hotel, gift, and restaurant bills and therefore estimate the likelihood of divorce".[128] Therefore, we cannot talk about a neutral data character. The presence or absence of data about a person may be the result of prejudice against him during the decision-making process. In addition, Al systems use data in a way that is often opaque, and statistical models may not allow liability for incorrect decisions. Many of these systems operate in a way that "abstracts any context surrounding [the system]."[129]

It is also important to note the autonomous aspect of AI functioning, i.e. the role of the human factor in the use of AI systems. If we describe AI-driven systems as decision-makers, then we have a view of the insignificance of human intervention in making a move, which can lead to

[126] Aaron Klein, *Reducing Bias in AI-based Financial Service, July 10, 2020*, Accessed February 11, 2023, URL:https://www.brookings.edu/research/reducing-bias-in-ai-based-financial-services/
[127] *Ibid*
[128] Darrel M. West, John R. Allen, *Turning Point: Policymaking in the Era of Artificial Intelligence*, Brookings Institution Press, 2020, p.8, URL:http://www.jstor.org/stable/10.7864/j.ctvwh8fcb.
[129] Andrew D Selbst, Danah Boyd, Sorelle A Friedler, Suresh Venkatasubramania, Janet Vertesi, *Fairness and Abstraction in Sociotechnical Systems*, January, 2019, 59-68, p. 59, URL:https://dl.acm.org/

dangerous assumptions. The author proposes a description of such systems as "recommended to make decisions." And thus, raising the prestige of human intervention in decision-making, thanks to the recommendatory nature of decisions made as a result of the use of AI systems. But while taking into account the human factor in decision-making, one must also pay attention to the diversity of people who develop and regulate financial technologies. Implicit biases of the programmer can penetrate the coding. In a 2018 interview, Timnit Gebru, co-founder of Black in AI [130] declared that diversity is crucial in Al because you need researchers that just have this social sense as a matter of course, not only in datasets.

Contrary to the opinion of Robert Bartlett Adair Morse Richard Stanton Nancy Wallace who did an investigation of the probability of discrimination in lending in face-to-face decisions or during algorithmic scoring in the paper “Consumer-lending discrimination in the FinTech era”. Assessing the extent of racial or ethnic discrimination in the largest consumer lending market, using the identification provided by the Mortgage Risk Assessment by Fannie Mae and Freddie Mac, found that "lenders charge Latin/African-Americans 7.9 and 3.6 basis points more. for the purchase and refinancing of mortgages, respectively, which costs them $ 765 million in total per year in the form of additional interest. " In addition, Latin American and African-American borrowers face greater barriers to obtaining a mortgage. Evidence shows that at least 6% of Latin American and African American applications are rejected, but they would have been accepted if the applicant did not belong to these minorities. This means rejecting up to 1.3 million applications from creditworthy minorities.

As for FinTech's algorithms, the rate of their discrimination is 40% less than face-to-face lenders. This is explained by the fact that FinTech lenders eliminate discrimination that arises from personal interaction between the initiators and borrowers. Thus, a lower level of discrimination with the use of FinTech algorithms suggests that eliminating personal interactions can reduce discrimination. Researchers also link the reduction of discrimination in lending to FinTech technology to the ease of applying and purchasing provided by the growth of FinTech platforms. To sum up, the benefits of using FinTech were highlighted:

- reducing discrimination;
- algorithmic lending, which increased competition or stimulated more purchases due to the simplicity of platform applications;

[130] Jackie Snow, *We're in a Diversity Crisis': Cofounder of Black in Al on What's Poisoning Algorithms in Our Lives*, February 14, 2018, Accessed March 5, 2023, URL:https://www.technologyreview.com/2018/02/14/145462/were-in-a-diversity-crisis-black-in-ais-founder-on-whats-poisoning-the-algo rithms-in-our/

- 0.74-1.3 million minority applications were rejected between 2009 and 2015 due to discrimination, but financial technology does not discriminate in approving loans.[131]

In turn, the researcher wants to express her support for the development of FinTech with the use of AI. Because technical progress is an inevitable phenomenon in modern society. The use of FinTech allows you to increase the scope of operational tasks and reduce their cost. This is undoubtedly attractive to customers and increases the popularity of one or another TPPs or PIs, which is favorable for the development of competition in the market. The appearance of open financing to replace the existing models of coexistence of TPPs and PIs is an absolutely logical continuation of the development of open banking, which was introduced in PSD2. The development and popularity of open financing are obvious. Expanding the scope of PSD2 will allow for wider use of FinTech, especially those that use AI technologies. This will reduce the factor of human influence and the occurrence of behavior that is characterized by discrimination and, as a result, provide more services and satisfy more customer needs, which in turn will lead to the growth of effective competition.

The most striking observation to emerge from the data analysis was the PSD2 does not apply for cryptocurrencies[132], one of the most prominent instances of FinTech in practice. In consideration of cryptocurrencies under EU payment services, the PSD2 applies to payment services, such as those that allow for the deposit of cash into a payment account and all associated operations; services that allow for cash withdrawals; the execution of payment transactions, such as transfers of funds between a user's payment service provider and other payment service providers; and the execution of payments where the funds are covered by a credit line for a payment service. According to PSD2, the transfer or management of funds/money and actions directed at it constitute the payment service. Payment services offered in the currencies of EU Member States and, under some circumstances, in the currencies of non-EU nations are covered by the PSD2. According to the PSD2, payments must be done in a currency that the parties have agreed upon. On this basis, the researcher concludes that cryptocurrencies are not currencies and the PSD2 does not apply to them. This is a significant omission because the use of cryptocurrencies was left out of the legislator's attention when adopting PSD2, which already indicates the inadequacy of PSD2 as a legal instrument for FinTech regulation. However, it is worth noting that the regulation of cryptocurrencies remains a subject of debate and should be one of the aspects of the PSD2 review. In favor of examining the application of FinTech in the light of provisions of the

[131] Robert Bartlett, Adair Morse, Richard Stanton, Nancy Wallace, Consumer-Lending Discrimination in the FinTech Era, June 2019, National Bureau of Economic Research, Cambridge, 42, URL:https://www.nber.org/system/files/working_papers/w25943/w25943.pdf

[132] Asress Adimi Gikay, *Regulating Decentralized Cryptocurrencies under Payment Services Law: Lessons from European Union Law*, Case Western Reserve Journal of Law, Technology and the Internet 9, 2018, 1-35.

PSD2, experts[133] have identified the strengths of traditional financial service providers, such as banks, compared to FinTech, including:

- many years of experience in the field of finance and trust;
- diverse access to services, including not only remote access but also personal contact and consulting services through a wide range of banking branches;
- a wide range of products and services offered to customers, which allows cross-selling and access to services provided by the bank's subsidiaries;
- as PSD2's obligation to provide access to customer account information, banks have the advantage that only they are allowed to provide customers to TPPs with mobile access in a regulated environment to their financial information, which includes not only bank accounts but also portfolio information, insurance contract and other products and services provided by the bank's subsidiaries.

The Directive provides additional opportunities for traditional financial service providers to:

- cooperation of the financial services industry with developers of FinTech, outsourcing of IT solutions to improve the quality of their products and services, and/or expanding the range of products by creating innovative financial products and services;
- increase business efficiency due to higher standardization, and as a result, reduce the cost of selected financial products and services;
- modernization of approaches to risk assessment based on modern methods of data analysis.

Regarding the weakness of traditional service providers:

- creating additional pressure on the banking margin through increased competition in financial services, as well as through stricter regulatory standards;
- potential partial loss of market share, especially in services such as payments, and loans;
- growing dependence of the bank on technological solutions of financial services that require additional investment in the internal IT infrastructure of the bank or require closer cooperation with developers of FinTech.

New threats have been identified, including:

- the need to change the business model for the implementation of innovations following changing conditions;

[133] *Supra note* 2

- an increase of operational risks due to the need to provide access to the information of the client's payment account;
- security risk when exchanging data with third-party payment providers;
- the risk of fraud in the case of dishonest third-party payment providers;
- the need to constantly increase investment in key IT systems to minimize ICT risks and data protection risks.

Thus, given the weaknesses and strengths of traditional suppliers under the Directive, it can be concluded that FinTech is both a real challenge for them and an opportunity for significant growth and promotion of services. The use of FinTech is an inevitable future for all traditional suppliers: it is, therefore, appropriate to invest and integrate new technologies into its business.

### 3.3. Summary

The main conclusion that can be drawn is that by opening access to accounts thanks to TPPs APIs, PSD2 gave an impetus to the development of open banking by giving traditional banks access to their databases for new technologies. TPPs are represented by 2 categories, namely PISP and AISP, the main difference of which is the ability to transfer funds. The use of FinTech with TPPs AI allows for reducing the level of discrimination.

Moreover, PSD2 created the conditions for the introduction and development of open banking, without which it is impossible to imagine our everyday life. The use of APIs and effective cooperation with TPPs allows banks to expand the list of their products and services and, as a result, improve the customer experience. The advantages of using open banking led to the creation of open financing. At the same time, the disadvantages of open banking are presented. In order to prevent and/or eliminate them, the competent authorities establish legal norms, which banks and TPPs effectively implement in their policies. Due to the broad interpretation of objectivity, proportionality, and non-discrimination behavior, provisions of PSD2 should be detailed in the new PSD3 for providing effective access for authorized TPPs with an aim to develop a competitive market of payment services.

## CONCLUSIONS

The research work presents a study on the literature and legal acts related to the analysis of the non-discrimination obligation of banks in providing payment services. The concept of data-sharing was included in the scope of Thesis as the part of the obligation to gain access to third-party payment providers which FinTech represents. Analyzing whether the legislative instruments declared by the PSD2 are sufficient to regulate non-discrimination duty on banks, the following statements can be concluded:

1. Evaluating FinTech as a tool for data-sharing, it can be highlighted its popularization and prospects due to its inherent qualities, among which are trust, decentralization, security, relatively reduced cost, speed, immutability, and individual control. Additional value of FinTech is that it creates a broad range of private and regulatory innovations made possible by the quick drop in computing costs, along with the widespread availability of dependable, high-speed connectivity (typically over the internet), and an explosion of newly collected data about a wide range of personal and professional traits and behaviors.

2. Data providers must grant access to their data to third parties in order to their further aggregation, analysis, and supply of new goods and services with an aim to establish effective competition. When examining the functioning EU market, it is clear from an analysis of the legal regulations on data sharing and the documents outlining the strategic development of this industry that due to high tempo of technical progress, the real issues are: incentives and data sharing initiatives; access to data; data portability with compatibility; technical requirements for ensuring data sharing.

3. The prohibition of discrimination is general for participants in all EU processes, including when payment services are provided. A broad interpretation of the exclusion of the discriminatory factor for objective, proportional, and legal reasons leads to a case in which it is difficult to foresee the abuse of PIs by these provisions and exclude discriminatory behavior on their part in practice. It is appropriate to specify the standards for objective, non-discriminatory, and proportionate access to third-parties. Companies should have explicit policies outlining the criteria for access as well as the circumstances under which access will be denied in order to determine the behavior of participants of payment services and allow for more effective settlement of conflicts between them.

4. Considering the impact of the PSD2 on the examples of some FinTech, it can be concluded that the provisions of the PSD2 cannot be applied or that there are obstacles due to its existence and establishment as one of the main legal instruments regulating payment services. Taking into account cryptocurrencies, the further development of PSD2 on this subject should be

made in order to eliminate gaps in the existing framework. On the other hand, the functioning of open banking in the EU is provided by PSD2 which aims to increase competition and innovation in payment services. The PSD2 creates conditions for the effective coexistence of "traditional" banks and FinTech in the future will lead to a qualitatively better level of service and create conditions for new innovative products and services, as well as reduce their costs. The remaining issues are subject to implementation norms of the PSD2 in national law and as a result, different approaches to using different regulations for the same payment service depending on the country of payment.

5. Currently, It would be appropriate to say that the protection of competition introduced and envisaged by PSD2 is under threat. As far as the principle of objectivity and proportionality are too broad and are interpreted by PIs in their way, it is important to specify provisions of the Articles 35 and 36 of PSD2 in PSD3. Such a specification will ensure that PSPs may be accessed in a proportionate, objective, and non-discriminatory manner since registered PSPs should not be subject to discrimination in the member states. Specifying the criteria for access and refusal of such will avoid disputes between the parties, and in the event of such conflict, a prompt and effective resolution will be granted.

## LIST OF BIBLIOGRAPHY

### Miscellaneous


1. Aaron Klein, *Reducing Bias in AI-based Financial Service, July 10, 2020, Accessed February 11, 2023, URL:*https://www.brookings.edu/research/reducing-bias-in-ai-based-financial-services/
2. Andrew D Selbst, Danah Boyd, Sorelle A Friedler, Suresh Venkatasubramania, Janet Vertesi, *Fairness and Abstraction in Sociotechnical Systems*, January, 2019, 59-68, p. 59, URL:https://dl.acm.org/
3. Angus McFadyen, *Key features of PSD2 and what they mean for the payments industry*, January 26, 2015, Accesses April 27, 2022, URL:https://www.pinsentmasons.com/out-law/analysis/key-features-of-psd2-and-what-they-mean-for-the-payments-industry
4. Arnaut C., Pont M., Scaria E., Berghmans A., Leconte S., *Study on data sharing between companies in Europe*, Luxembourg, Publications Office of the European Union p.vii; p. 2, URL:https://dl4ld.nl/KK0118016ENN.en.pdf
5. Asress Adimi Gikay, *Regulating Decentralized Cryptocurrencies under Payment Services Law: Lessons from European Union Law*, Case Western Reserve Journal of Law, Technology and the Internet 9, 2018, 1-35.
6. Ben Woolsey & Emily Starbuck Gerson in *The History of Credit Cards*, May 11, 2009, Accessed April 24, 2022, URL: http://www.creditcards.com/ credit-card-news/credit-cards-history-1264.php
7. BIS, *History of the Basel Committee, Accessed April 24*, 2022, URL: http://www.bis.org/bcbs/history.pdf.
8. Carol McDonald, *Big Data opportunities for Telecommunications*, November 5, 2020, Accessed April 22, 2022, URL: https://mapr.com/blog/big-data-opportunities-telecommunications/
9. Catarina Arnaut, Marta Pont, Elizabeth Scaria, Arnaud Berghmans, Sophie Leconte, *Study on data sharing between companies in Europe*, 2018, p.6. URL: https://dl4ld.nl/KK0118016ENN.en.pdf
10. C. Goettenauer, *"FinTech": in search of a legal definition,* April 12, 2021, Accesses April 26, 2022, URL: https://officialblogofunio.com/2021/04/12/FinTech-in-search-of-a-legal-definition/
11. Chaplius Halder & Co, Investment Advisory: The Rise of Robots, 2015, Accessed April 27, 2022, URL:http://investglass.com/images/press/Iivestmrent-Advisory-The-rise-of-the-Robots-Chappuis-Halder-InivestGlass.pdf

12. Chikako Baba, Cristina Batog, Enrique Flores, Borja Gracia, Izabela Karpowicz, Piotr Kopyrski, James Roaf, Anna Shabunina, Rachel van Elkan, Xin Cindy Xu, *FinTech in Europe: Promises and Threats*, IMF Working Paper, November 2020.
13. 13. Clinford Chance, *PSD2 implementation: What you need to know,* September 2017, p.7 https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2017/09/psd2-implementation-what-you-need-to-know.pdf
14. Congressional Research Service, *Open Banking, Data Sharing, and the CFPB's 1033 Rulemaking*, September 9, 2021, URL:https://crsreports.congress.gov/product/pdf/IN/IN11745
15. Crémer, J., de Montjoye, Y., Schweitzer, H., *Competition Policy for the digital era*, 2019, Luxembourg: Publications Office of the European Union, p. 76.
16. Danske Bank, *What is open banking?* Accessed November 10, 2022, URL:https://danskebank.com/about-us/openbanking
17. Darrel M. West, John R. Allen, *Turning Point: Policymaking in the Era of Artificial Intelligence*, Brookings Institution Press, 2020, p.8, URL:http://www.jstor.org/stable/10.7864/j.ctvwh8fcb.
18. Data Exchange, Data Sharing, Data Marketplace & Data Hub, *Data Exchange technology for data sourcing, acquisition & sharing*, Accessed June 28, 2022, URL: https://www.dawex.com/en/
19. Data Transfer Initiative, Accessed April 12, 2023, URL: https://datatransferproject.dev/
20. David Carse, *Symposium on Applied R&D: Enhancing Global Competitiveness in the Next Millennium*, October 8, 1999, URL: http://www.bis.org/review/r991012c.pdf
21. Douglas W. Arner; Janos Barberis; Ross P. Buckley, *The Evolution of FinTech: A New Post-Crisis Paradigm*, Georgetown Journal of International Law 47, no. 4 (Summer 2016), p. 1271-1320.
22. Electronic IDentification, *eIDAS: The Digital Identification Regulation for Europe*, May 12, 2022, Accessed November 18, 2022, URL:https://www.electronicid.eu/en/blog/post/eidas-regulation-electronic-signature/en
23. *Embracing open data is now more important than ever (open data note 2 of 2)*, June 24, 2021, Accessed April 23, 2022, URL:https://cms-lawnow.com/en/ealerts/2021/06/embracing-open-data-is-now-more-important-than-ever-open-data-note-2-of-2
24. European Banking Authority, Payment Institutions Register, Accesses November 15, 2022, URL:https://euclid.eba.europa.eu/register/pir/disclaimer?returnUrl=%2Fpir%2Fsearch

25. European Banking Federation, *Guidance for implementation of the revised Payment Services Directive*, 2019, URL:https://www.ebf.eu/wp-content/uploads/2019/12/EBF-PSD2-guidance-Final-December-2019.pdf
26. European Central Bank, The revised Payment Services Directive (PSD2) and the transition to stronger payments security, March, 2018, Accessed April 22, 2022, URL: https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html
27. European Commission, Directorate-General for Communications Networks, Content and Technology, Wauters, P., Siede, A., Cocoru, D., et al., *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability : final report*, Publications Office, 2018, pp. 15-16, URL:https://data.europa.eu/doi/10.2759/781960
28. European Commission, *Free flow of non-personal data*, Accessed April 12, 2023, URL:https://digital-strategy.ec.europa.eu/en/policies/non-personal-data
29. European Commission, *Questions & Answers on the Geo-blocking in the context of e-commerce, 2018*, 45, URL: https://www.eccireland.ie/wp-content/uploads/QuestionsAnswersontheGeo-blockingRegulationinthecontextofe-commerce.pdf
30. Euro Retail Payments Board, Report Next Phase of the ERPB WG on a SEPA API Access Scheme, June 28, 2021, 111, URL:https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/15th-ERPB-meeting/Report_from_the_ERPB_working_group_on_a_SEPA_API_Access_Scheme.pdf?52770756a713895bdc4fd072873346b
31. Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities*, June 27, 2017, URL: Retrieved from http://www.fsb.org/wp-content/uploads/R270617.pdf.
32. Financial Stability Board, *FinTech and market structure in financial services: Market developments and potential financial stability implications*, February 2019, Accesses April 27, 2022, URL: http://www.fsb.org/2019/02/FinTech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability- implications/.
33. George Walker, *International Banking Regulation Law, Policy and Practice*, 2001.
34. Giancarlo Barbiroli, *The Dynamics of Technology: a Methodological Framework for Techno-economic Analyses*, 1997, Dordrecht (Netherlands); Boston: Kluwer Academic. Theory and decisions library. Series A. Philosophy and methodology of the social science, v.25. p.317-331.
35. How to Crack a Nut, *New CJEU Case Law Against Excessive Disclosure: Quid de Open Data?* (C-54/21, AND JOINED C-37/20 AND C-601/20), November 22, 2022, Accessed

April 16, 2023, URL:https://www.howtocrackanut.com/blog/2022/11/22/cjeu-case-law-against-excessive-disclosure-quid-de-open-data

36. Howell Edmunds Jackson, The Nature of the FinTech Firm and its Implications for Financial Regulation, July 15, 2020, p.9, URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3659503
37. Hudson Harris, *hiQ v. LinkedIN - Who Controls Your Publicy Available Data?*, January 7, 2018, Accessed April 12, 2023, URL: https://www.tripwire.com/state-of-security/featured/hiq-v-linkedin-controls-publicly-available-data/.
38. Hunton Anderws Kurth's, *CJEU Restricts Indiscriminate Access to Electronic Communications for National Security Purposes,* October 12, 2020, Accessed April 12, 2023. URL: https://www.natlawreview.com/article/cjeu-restricts-indiscriminate-access-to-electronic-communications-national-security
39. Jackie Snow, *We're in a Diversity Crisis': Cofounder of Black in Al on What's Poisoning Algorithms in Our Lives*, February 14, 2018, Accessed March 5, 2023, URL:https://www.technologyreview.com/2018/02/14/145462/were-in-a-diversity-crisis-black-in-ais-founder-on-whats-poisoning-the-algo rithms-in-our/
40. Jack Wilson, *Explaining changes to the 90 day rule for open banking access,* February 14, 2022, Accessed February 6, 2023, URL:https://truelayer.com/blog/explaining-changes-to-the-90-day-rule-for-open-banking-access/
41. Jack Wilson, PSD2 4 years on: why open banking is a success - and how to judge it, January 13, 2022, Accessed November 20, 2022, URL:https://truelayer.com/blog/psdon2-4-years-on-why-open-banking-is-a-success-and-how-to-judge-it/
42. Jan Krämer, Daniel Schnurr, Alexandre de Streel Project Report, Internet Platforms and Non-Discrimination, December 5, 2017, URL: https://euagenda.eu/upload/publications/untitled-121136-ea.pdf
43. Jerry W. Markham,*From Christopher Columbus to the Robber Barons: A Financial History of the United States 1492–1900* (1st ed.), 2002, Routledge.
44. Jill Hills, *The struggle for control of global communication: the formative century,* 2002, Urbana, USA University of Illinois Press.
45. John Cassels. *What is FRAND?,* August 23, 2013, Accessed April 6, 2023, URL:https://www.fieldfisher.com/en/insights/what-is-frand
46. Joris Toonders, *Data Is the New Oil of the Digital Economy*, Accessed April 22, 2022, URL: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/
47. Inge Graef, Martin Husovec, Jasper van den Boom, "*Spill-overs in data governance: Uncovering the uneasy relationship between the GDPR's right to data portability and EU*

*sector-specific data access regimes*", Journal of European Consumer and Market Law Volume 9, Issue 1 (2020) pp. 3-16.

48. Inna Romānova, Simon Grima, Jonathan Spiteri, Marina Kudinska, *The Payment Services Directive II and Competitiveness: The Perspective of European FinTech Companies*, European Research Studies Journal Volume XXI, Issue 2, 2018, pp. 3 - 22.
49. International Monetary Fund, *FinTech: the Experience so far*, IMF Policy Paper, June, 2019, p.5.
50. International Organisation of Securities Commissions. *IOSCO Research Report on Financial Technologies (FinTech)*, February 2017, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf.
51. Kimberley Moran, *PSD2 in review*, July 5, 2022, Accessed February 6, 2023, URL:https://plaid.com/blog/psd2-in-review/
52. Mario Palmieri, *Open Banking PSD2 regulation in EU*, July 14, 2022, Accessed November 21, 2022, URL:https://FinTechlegal.center/open-banking-psd2-regulation-in-the-eu/
53. Mary K. Pratt, *Top 10 benefits of blockchain technology for business*, June 2, 2021, Accessed April 27, 2022, URL: https://www.techtarget.com/searchcio/feature/Top-10-benefits-of-blockchain-technology-for-business
54. Matthew Blenkarn, *What does AISP & PISP mean?*, March 9, 2022, Accessed November 20, 2022, URL:https://truelayer.com/blog/what-does-aisp-pisp-mean/
55. Matthew Rowlinson, *Real Money and Romanticism*. Cambridge, 2010, Cambridge University Press.p.7.
56. Matthias Leistner, Lucie Antoine, *IPR and the use of open data and data sharing initiatives by public and private actors*, May, 2022, European Union, p.25, URL:https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf
57. Nadja van der Veer, *Taking a chance on TPPs: a road banks cannot afford to follow*, September 20, 2019, Accessed November 10, 2022, URL:https://paymentsguru.eu/taking-a-chance-on-tpps-a-road-banks-cannot-afford-to-follow/
58. Nadja van Der Veer, *Why gaps in the EBA Register leave worries over security*, July 19, 2019, Accessed November 10, 2022, URL:https://paymentsguru.eu/why-gaps-in-the-eba-register-leave-worries-over-security/
59. Niels Vandezande, *EDPB Clarifies the Interplay Between GDPR and PSD2*, February 15, 2021, Accessed September 22, 2023, URL:https://www.timelex.eu/en/blog/edpb-clarifies-interplay-between-gdpr-and-psd

60. OECD, *Financial Markets, Insurance and Private Pensions: Digitalisation and Finance*, 2018, p.3.
61. Open Bank Project, *Open Banking API Platform. What is the Open Bank Project Platform?*, Accessed November 18, 2022, URL:https://www.openbankproject.com/openbankingmiddleware/
62. Par Dipak Dasgupta, *Financial Innovation and the State: Lessons for 21st Century Climate FinanceFrom the 19th Century Railway Era,* October 1, 2015, Accessed April 25, 2023, URL: http://www.cepii.fr/ blog/bi/ post.asp?IDcommunique 407.
63. Patrick Thibodeau, *TI's First Handheld Calculator Is Now a Museum Piece,* September 26, 2007, Accessed April 25, 2023, URL: http://www.computerworld.com/article/2541155/computer-hardware/ti-s-first-handheld-calculator-is-now-a-museuin-piece.html.
64. Paul Langley & Andrew Leyshon, *The Platform Political Economy of FinTech: Reintermediation, Consolidation and Capitalisation,* New Political Economy, 26:3,2021, p. 376-388.
65. Paul Volcker, *The Only Thing Useful Banks Have Invented in 20 Years is the ATM,* December 13, 2009, Accessed April 22, 2022, URL: http: //nypost.con/2009/12/13/the-only-thing-useful-banks-have-inivenited-ini-20-years-is-the-atm/.
66. Ravi Menon, *FinTech: Harnessing its Power, Managing its Risks*, April 2, 2016, URL: http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/FinTech-Harnessing-its-Power-Managing-its-Risks.aspx.
67. Richard A Buckley, *Negligence - when does a duty of care arise?,* Accessed November 11, 2022, URL:https://www.lexisnexis.co.uk/legal/guidance/negligence-when-does-a-duty-of-care-arise
68. Robert Bartlett, Adair Morse, Richard Stanton, Nancy Wallace, Consumer-Lending Discrimination in the FinTech Era, June 2019, National Bureau of Economic Research, Cambridge, 42, URL:https://www.nber.org/system/files/working_papers/w25943/w25943.pdf
69. R. Rupeika-Apoga, E. I. Thalassinos, *Ideas for a Regulatory Definition of FinTech*, International Journal of Economics and Business Administration Volume VIII, Issue 2, 2020, pp. 136-154.
70. Sara Heegaard, *What is a payment API?,* August 31, 2021, Accesses November 19, 2022, URL:https://rechargepayments.com/glossary/payment-api/
71. SEON, *What is Strong Customer Authentication (SCA)?*, Accessed November 20, 2022, URL:https://seon.io/resources/dictionary/sca/

72. SHIP Global IP, *FRAND licensing and why is so important for technical standards*, November 13, 2019, Accessed April 12, 2023. URL:https://shipglobalip.com/blog/frand-licensing-and-why-is-so-important-for-technical-standards-
73. Skeps, *The Importance of FinTech In The Post-COVID World*, June 2, 2020, Accessed May 19, 2022, URL: https://www.skeps.com/blog/the-importance-of-FinTech-in-the-post-covid-world
74. Statista Research Department, *Open banking users worldwide in 2020 with forecasts to 2024, by region*, 31 May, 2022. Accesses November 18, 2022, URL:https://www.statista.com/statistics/1228771/open-banking-users-worldwide/
75. Stax, *Payment APIs: What Are They and How do They Work?* Accessed November 19, 2022, URL:https://staxpayments.com/blog/payment-apis-how-they-work/
76. StJohn Deakins, *Data Is The New Water: Seven Reasons Why*, October 12, 2017. Accessed April 22, 2022. URL: https://www.huffingtonpost.co.uk/stjohn-deakins-195/data-is-the-new-water-sev_b_18228184.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKFyRrFQktwDM_6MAdftvjuPQDCEadvytk8GAGhl6AwPo8yhhNIJCcRnbn-IkApnCLitJ6slcVbT6GzLikwW5Nm6VPN_XJV5Ki8729_W7Wl-w2cmnu7R5db4Enx2HkMn35LniJSB2v2eyVW-Un_lpjobXbklb0-c7RXBlQ6iwsqs
77. *SWIFT History*, Accessed April 24, 2022, URL: https://www.swift.con/about-us/history
78. The Bali FinTech Agenda, *IMF Policy Paper*, October 2018, p.7.
79. The Economist, *The world's most valuable resource is no longer oil, but data*, May 6, 2017, Accessed April 22, 2022, URL:https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
80. The European Commission, Report/ Study The European data market study update, July 6, 2020, Accessed April 25, 2022. URL: https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update
81. The European Data Protection Board, *One-Stop-Shop Leaflet*, June 29, 2021, Accessed April 13, 2023. URL: https://edpb.europa.eu/our-work-tools/our-documents/one-stop-shop-leaflet_en
82. The Expert Group for the Observatory on the Online Platform Economy, *Work stream on Data*, Accessed April 6, 2023, URL: https://platformobservatory.eu/app/uploads/2020/07/ProgressReport_Workstream_on_Data_2020.pdf

83. The investopedia Team, *Open banking: Definition, How it Works, and Risks*, April 4, 2022, Accessed November 19, 2022, URL: https://www.investopedia.com/terms/o/open-banking.asp
84. Thomas LaRock, *"Data is the New Oil", But That Also Means it Can be Risky*, October 6, 2022, Accessed April 6, 2023. URL:https://www.dbta.com/Columns/Next-Gen-Data-Management/Data-is-the-New-Oil-But-That-Also-Means-it-Can-be-Risky-155275.aspx#:~:text=British%20mathematician%20Clive%20Humby%20famously,growth%20to%20reach%20their%20goals
85. Wagennar Lawyer, *Duty of Care Banks*, January 2, 2017, Accessed November 11, 2022, URL:https://www.wagenaarlawyers.nl/en/termination-credit-agreement/
86. Your Europe, *Electronic and cash payments*, June 6, 2022, Accesses, November 10, 2022, URL:https://europa.eu/youreurope/business/finance-funding/making-receiving-payments/electronic-cash-payments/index_en.htm
87. Zvi Bodie, Robert C. Merton, *Finance*, 2000, Prentice Hall, 479 p.

**Documents and Legal Acts**

1. *Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions*, Official Journal of the European Union, October 27, 2000, p.0039-0043
2. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, Official Journal of the European Union 201, July 31, 2002, p. 0037-0047, URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN
3. *Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market*, Official Journal of the Europe Union, 376, p. 36-38.
4. *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance)*, Official Journal of the European Union, December 5, 2007, p. 1-36
5. *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing*

*Directive 2007/64/EC,* Official Journal of the European Union 337, December 23, 2015, p.35-127.

6. *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC*, Official Journal of the European Union, 141, p. 73-117
7. *Directive (EU) 2019/1024 of The European Parliament and of The Council of 20 June 2019 on open data and the re-use of public sector information,* Official Journal of the European Union 172, June 26, 2019, p.56-83.
8. European Commission, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, May 6, 2015, URL:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN
9. European Commission, *A European strategy for data*, COM(2020) 66 final, February 19, 2020, URL: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf
10. European Commission, *Building a European Data Economy*, COM(2017) 9 final, January 10, 2017, URL:https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy
11. European Commission, *Inception Impact Assessment Data Act,* Ref. Ares(2021)3527151, 28 May 2021, p. 1.
12. European Commission, *Staff Working Document on the free flow of data and emerging issues of the European data economy accompanying the Communication "Building a European data economy" (SWD(2017) 2 final), p. 25*, 2017, URL: https://ec.europa.eu/digital-single- market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy
13. European Commision, Commission Staff Working Document: *With a view to establishing guidance on the application of Article 20(2) of Directive 2006/123/EC on services in the internal market ('the Services Directive') Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the implementation of the Services Directive: A partnership for new growth in services 2012-2015*,June 8, 2012, URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012SC0146

14. European Commission, *Towards a thriving data-driven economy*, COM (2014) 442 final, June 2, 2014, URL:http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=6210.f
15. Financial Conduct Authority. *Principles for Business. Chapter 2. The Principles*, January 3, 2018, URL:https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html
16. Judgement of the Court of Justice of 12 January 2023, *RW v Österreichische Post*, C-154/21, EU:C:2023:3, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CJ0154&from=en
17. *Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (Text with EEA relevance)*, Official Journal of the European Union 123, May 19, 2015, p. 1-15.
18. *Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC*, Official Journal of the European Union 60I, March 2, 2018, p. 1-15.
19. *Regulation (EU) No 910/2014 of the European Parliament and Council of July 23, 2014 on electronic identification and trust services for electronic transaction in the internal market and repeating Directive 1999/93/EC*, Official Journal of the European Union, 257, August 28, 2014, p. 73-114.
20. *Revised Rules for Payment Services in the EU*, December 6, 2021, URL:https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

## ABSTRACT

This paper outlines the notion of sharing data and the obligation to grant access to third parties as a component of the non-discriminatory duty in the B2B sector with an aim to provide effective competitiveness declared by the EU.

The Thesis provides an analysis of the obligation of non-discrimination on banks as well as the mechanism of its implementation which is granted by PSD2. The research is based on guidelines of the European Commission, European Data Protection Board, CJEU practice, and reports of expert groups. The study's objectives include examining the current situation and issues, as well as potential solutions to strengthen the law against discrimination against FinTech while taking into consideration both the difficulties of the present and the challenges of the future.



**Keywords**: FinTech, data-sharing, discrimination, third parties, access to the system.

## SUMMARY

The master's thesis is focused on the issue of granted access from banks for third-party providers represented by FinTech. The thesis analyzes the practical application of the obligation, its current benefits, and its disadvantages. Also, based on the providing research on the previous practice collaboration between banks and FinTech, the study considers the future challenges of such data sharing while providing payment services in the future.

The Thesis is structured in 3 parts, each of which displays a certain obligation:

1. Data-sharing and access to the system as general fundamentals for non-discrimination;
2. The granted access to the bank's system for FinTech;
3. FinTech as a third-party player.

Each chapter includes a broad description of a specific responsibility, which is essential for the study of the banks' non-discrimination obligations that follows. The first part contains general consideration of the duty of data-sharing in the B2B sector. The second part analyzes FinTech as an instrument of providing such data exchange and its legal regulation by existing EU legislation including PSD2. The third part, explains the collaboration between banks and FinTech as a service provider under conditions provided by PSD2. Also, a particular chapter approves the practical significance of cooperation for the future development of the single EU market, in particular the sector of providing payment services and supporting the effective competitiveness among its participants.

The objectives of the Thesis are reflected and formulated as follows:

1. Evaluation of the development of FinTech's use in financial transactions, ascertain its legal status, and assess how well it complies with current legal requirements;
2. To assess the present state of the practice of data-sharing as a component of the private sector's non-discrimination obligation and how it relates to banks and FinTechs in the EU offering payment services.

Based on the conducted research, third parties, including users, government organizations, rival companies, and non-competing businesses, should be granted access to data sharing for their continued data gathering, analysis, and delivery of new goods and services. Consequently, it provides effective competitiveness within the EU which is declared by its strategy. It was concluded that the popularity of fintech as an instrument for data sharing is due to its intrinsic properties, including trust, decentralization, security, relatively low cost, speed, immutability, and individual control. For all participants of payment services discrimination is prohibited. The consolidation of PSD2 with other EU regulations, as well as its detailing and

forgiveness of the exclusion of the discriminatory factor for objective, proportional, and legal reasons, are additional factors that help determine the behavior of payment service participants and enable a more efficient resolution of disputes between them. It was determined that PSD2 does not apply to all types of FinTech, for example, cryptocurrencies are out of the scope of the studies Directive. Currently, the principle of objectivity and proportionality are too broad and are interpreted by PIs in their way and accordingly, it is challenging to anticipate how these provisions, which prohibit discriminatory conduct may be abused by PIs.

The main conclusion that can be drawn is that it is crucial to expand PSD2's Articles 35 and 36 in PSD3. Since registered PSPs should not be subject to discrimination in the member states as well as such a specification will guarantee that PSPs may be accessed in a proportionate, objective, and non-discriminatory manner. The parties will not conflict if the conditions for access and rejection are clear, and if they do, a timely and satisfactory settlement will be provided.