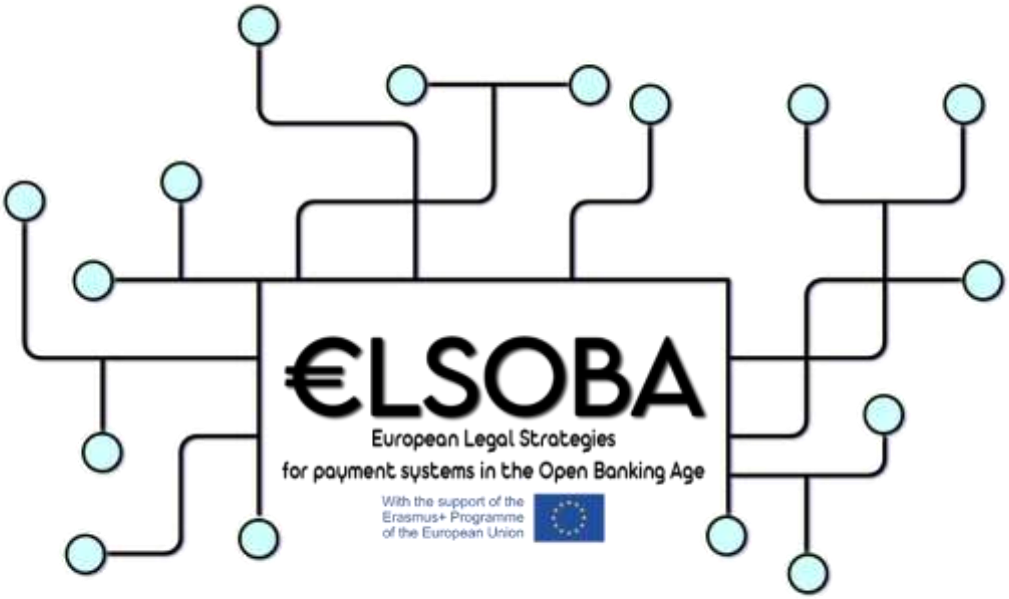

Materials

on

Open Banking

1. Alessandro Palmieri

The Open Banking Movement and the Access to Accounts Rule: Challenges for Competition and Data Protection Law

2. Alessandro Palmieri, Blerina Nazëraj

Open Banking and Competition: An Intricate Relationship

THE OPEN BANKING MOVEMENT AND THE ACCESS TO ACCOUNTS RULE: CHALLENGES FOR COMPETITION AND DATA PROTECTION LAW

Alessandro Palmieri[1]

DOI: https://doi.org/10.24040/pros.13.11.2020.svp.222-232

Abstract

The global development of open banking regulations and initiatives, while promising benefits to individuals and small businesses, raises also several concerns. This entry, focusing on the European Union experience, addresses some critical issues not only in respect to the defence of consumers' economic interests, but also, and mainly, with regard to the safeguard of customers' personal data and the maintenance of an adequate level of competition in the relevant markets. The author advocates a revision of the existing protecting devices or, alternatively, the creation of new mechanisms, more suitable to ensure a high level of protection for the interests at stake.

Keywords

Open banking, payment services, consumer protection, competition, data protection

Introduction

The open banking movement is at the centre of a worldwide debate. Several legislatures, at the national as well as the supranational level, have taken significant steps towards implementing an efficient open banking regime, susceptible of being, as a first approximation, described as a system under which banks open up their application programming interfaces (APIs) for third parties[2].

The process of implementation of open banking raises many legal questions, related to different branches of law. Indeed, since the first stage of its development, open banking,

[1] Prof. Dr. Alessandro Palmieri, PhD., University of Siena, Department of Law.
[2] According to P. Gupta and T.M. Tham, *Fintech. The New DNA of Financial Services*, de Gruyter, 2019, 157, consists in the «adoption of common standards for collaboration between banks and other players within the banking ecosystem».

alongside the expected benefits, has revealed critical issues, which demand the attention of academics and other experts from various areas of law. In this context, one may come across issues that pertain to private law: more specifically, focus shall be put on consumer protection, personal data privacy and the safeguard of competition. A large part of the difficulties stem from one of the core features of the open banking system, that is to say from the "access to account rule", according to which financial institutions are obliged to allow third parties to obtain customers' account data on the basis of customers' consent.

Open banking as a global phenomenon: a window on non-European experiences

As it has been pointed out in the relevant literature, open banking "is proving to be a global phenomenon"[3]. Before concentrating on European Union, it seems useful to conduct a survey of non-European experiences.

It is extremely remarkable the way Australia has dealt, and keeps on dealing, with open banking, in the framework of a more ambitious project that aims at enhancing an open-data landscape. In July 2020, the Australian Consumer Data Right Act came into force, which pursues the goal of improving competition and choice, as allows that transaction data, customer data and product data can be communicated with third party comparison sites to increase the consumer's negotiation power. The scope of this piece of legislation is very broad: in the initial stage, it is applicable only in the banking sector; then it will apply to the energy and telecommunications sectors, before including gradually other industries on a sector-by-sector basis. It is also of interest what is taking place in Brazil. In May 2000, the Central Bank of Brazil (Banco Central do Brasil) has issued a regulation on the implementation of open banking. Like similar attempts to govern the phenomenon, the said regulation – which defines open banking as a standardized sharing of data and services through the opening and integration of systems – aims at encouraging innovation, promoting competition, and increasing the efficiency of the national financial system.

Other legal systems are preparing the adoption of the open banking paradigm. One of these is Canada where, in June 2019, the Senate Committee on Banking, Trade and Commerce

[3] See, for instance, B. Regnard-Weinrabe and J. Finlayson-Brown, *Adapting to a changing payments landscape*, in J. Madir (ed.), *FinTech. Law and Regulation*, Edward Elgar, 2019, 41.

asked the Government to take immediate steps to initiate an open banking framework. More recently, in January 2020, the Advisory Committee on Open Banking, appointed by the Ministry of Finance, determined that the benefits of open banking outweigh its cost. In its report the Committee observed that a robust consumer-directed framework: 1) could give consumers greater control of their information; 2) could support a more innovative and competitive sector by setting rules and protections around data use and requiring data to be transferred in a more secure form. After the publication of this report, a new phase commenced in the design of an open banking regulatory framework. Currently the focus is on determining how regulators and the financial sector can mitigate data security and privacy risks. Something noteworthy is happening in the United States where, as of today, consumers' access to financial data sharing has been largely dependent on private-sector efforts. Indeed, Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (passed in the aftermath of the financial crisis of 2008) provides that, subject to rules prescribed by the Bureau of Consumer Financial Protection (CFPB), a consumer financial services provider must make available to a consumer information, in its control or possession, concerning the consumer financial product or service that the consumer obtained from the provider. This provision, which dates bakes to 2010, has never been implemented. But, on 22 October 2020, the CFPB has announced its intention to regulate open banking, issuing an advanced notice of proposed rulemaking.

It shall be noted that other countries – including India, Japan, Singapore and South Korea – still rely on market mechanisms as levers to support the growth of open banking and the effectiveness of data sharing measures.

The access to account rule in the EU system

European Union is widely regarded as the frontrunner of the above said global tendency, due to the fact that its decisive move to reach the mentioned goal dates back to 2015, when the Directive (EU) 2015/2366, on payment services in the internal market (known as "PSD2") was enacted. And, more recently, EU seems to have taken the lead in the ambitious road towards open finance. As a matter of fact, in the context of the "Digital Finance Strategy", launched in September 2020, the European Commission announced that, by 2024, the EU should have an open finance framework in place, in line with the EU Data Strategy, the upcoming Data Act,

and Digital Services Act. The concept of open finance goes beyond open banking because it involves the sharing and use of customer-permissioned data by banks and third-party providers to create new services.

One of the crucial factors in the context of PSD2 is the "access to accounts rule" (often labelled as "XS2A").

Speaking of this rule, several provisions of the Directive are relevant. First, one has to take into account Article 36 ["Access to accounts maintained with a credit institution"] which states that: "Member States shall ensure that payment institutions have access to credit institutions' payment accounts services on an objective, non-discriminatory and proportionate basis. Such access shall be sufficiently extensive to allow payment institutions to provide payment services in an unhindered and efficient manner. The credit institution shall provide the competent authority with duly motivated reasons for any rejection".

Then, one encounters two other provisions devoted, respectively, to payment initiation services (Article 66, entitled "Rules on access to payment account in the case of payment initiation services") and to account information services (Article 67, entitled "Rules on access to and use of payment account information in the case of account information services").

According to paragraph 1 of Article 66, "Member States shall ensure that a payer has the right to make use of a payment initiation service provider to obtain payment services […]. The right to make use of a payment initiation service provider shall not apply where the payment account is not accessible online". The supply of the payment initiation service inevitably requires that the third-party providers shall have access to some of the payment service user's data, and the ability to store them. But, in this regard, the EU legislature has introduced some limits; the payment initiation service provider is prevented from: 1) storing sensitive payment data of the payment service user (paragraph 3, lett. e); 2) requesting from the payment service user any data other than those necessary to provide the payment initiation service (paragraph 3, lett. f); 3) using, accessing or storing any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer (paragraph 3, lett. g)[4].

Furthermore, according to paragraph 1 of Article 67, "Member States shall ensure that a payment service user has the right to make use of services enabling access to account

[4] Axccording to B. Geva, *Payment Transactions under the E.U. Second Payment Services Directive – An Outsider's View*, 54 Tex. Int'l L.J. 211, 220 (2019), regulatory standards favor the indirect acces mode, where the Account Servicing Payment Service Provider provides the Payment Initiation Services Provider (PISP) account access through a dedicated application interface, because this mode is capable of limiting the data accessed by the PISP to only what is required for the provision of the service

information […]. That right shall not apply where the payment account is not accessible online". In addition, paragraph 2, lett. a), specifies that the account information service provider shall "provide services only where based on the payment service user's explicit consent".

Concerns for consumers' interests, data protection and competition in the marketplace

The access to account rule could have an adverse impact not only on the economic interests of consumers and other weak parties (such as microenterprises), but also on customers' data protection as well as on the competitiveness of the market as a whole.

Among the most serious dangers, one has to mention unauthorized payments or transactions made without the account holder's permission and defective payments or transactions, requested by the customer but wrongly processed by the providers involved. Concerns have also been raised about the information obligations that payment service providers should fulfil toward payment service users in respect to the payment service contract and payment operations. Regardless of the fact that the EU legislation sets out a package of rules designed to foster transparency, improving the information requirements, especially devoted to framework contracts and payment transactions subject to such contracts, which are of greater economic importance than singular payment transactions [arts. 38 et seq. PSD2], these rules must be placed in their proper position in the general framework of consumer protection law.

However, the specific problems affecting the consumer as payer have been addressed in 2019 by European Court of Justice in the *Verein für Konsumenteninformation* judgment[5]. On that occasion, the ECJ was asked to clarify the scope of provisions that were not immediately linked to consumer protection, since they were instead related to the technical and business requirements for credit transfers and direct debits [Regulation 260 of 2018]; nevertheless, it provided a favourable interpretation for consumers, imposing a ban on discrimination between different classes of purchasers. If this judgment proves to be the expression of a lasting trend, this will lead to enhance the protection of payers. As I have noted elsewhere, usually consumers in the digital environment combine the roles of buyers and payers; so, making stronger the

[5] ECJ 5 September 2019 [ECLI:EU:C:2019:673].

position of the payers will likely result in an overall enhancement of the digital consumers' economic welfare.

Other crucial issues are raised by the intersection between the open banking business model and data protection principles. Several risks are related to the processing of personal data connected to the provision of the services in this new business environment. It seems necessary to eliminate the inconsistencies between the sector-specific rules and the provisions set out by the General Data Protection Regulation (GDPR). Useful elucidations are offered in the "Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR", adopted by the European Data Protection Board (EDPB) on 17 July 2020. In particular, in that document, the EDPB expressed its view on the nature of the explicit consent of the payment service user required by some significant provisions of PSD2, specifying that consent under PSD2 is different from consent under GDPR, because the first one is deemed to be an additional requirement of a contractual nature.

Under the GDPR, consent serves as one of the six legal grounds for the lawfulness of processing of personal data. Article 4 (11) of the GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". These four conditions –freely given, specific, informed, and unambiguous– are essential for the validity of consent. The EDPB has recently specified (in its Guidelines 05/2020 on consent under Regulation 2016/679), that consent can only be an appropriate lawful basis if a data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. Moreover, according to Article 9 of the GDPR, consent is one of the exceptions from the general prohibition for processing special categories of personal data. However, in such case the data subject's consent must be 'explicit'. This means that the data subject must give an express statement of consent for specific processing purpose or purposes. Although the consent mentioned in PSD2 is not a legal ground for the processing of personal data, this consent is specifically related to personal data and data protection, and ensures transparency and a degree of control for the payment service user. It is interesting to observe that the EDPB added that the payment service user must be able to choose whether to use the service and cannot be forced to do so. Therefore, the consent under PSD2 must be a freely given consent too.

In terms of data protection law, it has to be recalled also the principle of data minimisation, according to which third-party providers should collect only personal data necessary to provide the specific payment services requested by the payment service user. Since financial data may contain references to all aspects of a data subject's private life, it is necessary to find out the best strategies that can be developed to avoid data breaches (just think of the consequences of giving untrusted parties access to log-in credentials) or, when a breach occurs, to grant an effective remedy to persons whose fundamental rights have been violated.

Furthermore, one has to consider that the judgment of the ECJ in the *Facebook Ireland and Schrems* case[6] (which has declared invalid the Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-US Privacy Shield) may influence the processing of personal data carried out for the purposes of open banking, since a meaningful number of Account Information Service Providers and Payment Initiation Services Providers, are located outside the EU. The ECJ has made clear that GDPR provisions apply to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.

Although one of the purposes of the rules enacted at the European level is to increase competition and openness between banks and non-banking institutions, antitrust issues may arise from the business conduct of the various operators. It is particularly important to make competition work in a sector where some players (namely, Big-Tech firms), leveraging on their skills in the field of data analytics, may acquire a dominant position, which in the end could result in a welfare loss for consumers.

[6] ECJ 16 July 2020 [ECLI:EU:C:2020:559]. In that circumstance, the Court held also that Article 46(1) and Article 46(2)(c) of the GDPR «must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation». On the *Facebook Ireland and Schrems* judgment, see M. Rotenberg*, Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection*, in *European Law Journal*, 2000, vol. 26, 1-2, 141-152; A. Chander, *Is Data Localization a Solution for Schrems II?*, in *Journal of International Economic Law*, 2000, vol. 23, 3, 771-784.

In the light of the provisions concerning the access to, and the use of, data relating to online payment accounts, many aspects have to be clarified from a competition law point of view: among the others, the definition of the relevant markets; the identification of the dominant entities; the relationship with the essential facility doctrine.

With respect to this specific point, many observers are fearful about the effects of the entry into the market of the so-called Big-Tech giants. An interesting proposal of reform, which aims at rebalancing power relations between the different parties, is centred in the idea that a reciprocity clause shall be added to the rules currently in force, so that not only third-party providers would be able to access bank customers' data, but also banks should be entitled to access all data stored by the said providers pertaining to the same customers[7].

Specific tools have to be designed in order to prevent the monopolization of the market by Big-Tech firms, which may leverage on their ability to tailor their services around customers' needs, to exploit economies of scope, and to cross-subsidise their services with the ones they offer in other markets. The competition problems encountered in the financial sector need to be inscribed in the framework of the more general debate around access to data in the digital sphere.

Civil liability rules can play a significative role in this context, to the extent that they are able to compensate those who have sustained losses as a result of unlawful conducts of banks, financial institutions, Account Information Service Providers and Payment Initiation Services Providers, as well as to deter further infringements.

Conclusion

According to an article recently published in is an international journal of technology law, the analysis of PSD2, and of the Regulatory Technical Standards adopted by the Commission, shows that the goal to develop the market for payment services has a higher priority; security and privacy are ultimately subordinate[8]. Analogous concerns can be raised with respect to the safeguard of a fair and vibrant competition in the relevant markets.

[7] F. Di Porto, G. Ghidini, ''I Access Your Data, You Access Mine'': Requiring Data Reciprocity in Payment Services, in International Review of Intellectual Property and Competition Law - IIC, 2020, 51, p. 307-329.
[8] See P.T.J Wolters, B.P.F. Jacobs, *The security of access to accounts under the PSD2*, in *Computer Law & Security Review*, 2019, 35, p. 29-41.

Since we are already in the 'open banking age' (at least in an early stage of it), and we are approaching the 'open finance age', scholars and other experts are called to explore new paths in order to minimise the mentioned risks, trying to adapt the existing protecting devices or to create new mechanisms, more suitable to face such important challenges as we are doing nowadays. These tools should increase the overall security of digital transactions and ensure a high level of protection to consumers and other vulnerable parties.

BIBLIOGRAPHY

ARNER D.W., ZETZSCHE D.A., BUCKLEY R.P., WEBER R.H.: Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II, in Standard Journal of Law Business and Finance, 2020, vol. 25, 245-288.

BORGOGNO O., COLANGELO G.: Data, Innovation and Competition in Finance: The Case of the Access to Account Rule, in European Business Law Review, 2020, 31, no. 4, 573-610.

BORGOGNO O., COLANGELO G.: The data sharing paradox: BigTechs in finance, May 28, 2020, available at SSRN: https://ssrn.com/abstract=3591205 or http://dx.doi.org/10.2139/ssrn.3591205 (forthcoming in European Competition Journal).

BURDON M., MACKIE T.: Australia's Consumer Data Right and the Uncertain Role of Information Privacy Law, in International Data Privacy Law, 2020, 10(3), 222-235.

CHANDER A.: Is Data Localization a Solution for Schrems II?, in Journal of International Economic Law, 2000, vol. 23, 3, 771-784

CIRAOLO F.: Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti", in Rivista di diritto bancario, 2020, 611-650.

DE PAOLI D.: PSD2 e privacy, in M.C. Paglietti, M.I. Vangelisti (eds.), Innovazione e regole nei pagamenti digitali il bilanciamento degli interessi nella PSD2, Roma TrE-Press, 2020, 147-151.

DI PORTO F., GHIDINI G.: ''I Access Your Data, You Access Mine'': Requiring Data Reciprocity in Payment Services, in International Review of Intellectual Property and Competition Law - IIC, 2020, 51, 307-329.

GAMMALDI D., IACOMINI C.: Mutamenti del mercato dopo la PSD2, in Maimeri F., Mancini M. (eds.), Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute

e rivoluzione digitale, Quaderni di Ricerca Giuridica della Consulenza Legale, Banca d'Italia, 2019, no. 87, 123-142.

GAUCI R.: Is Europe a Good Example of Open Banking?, in S. Chishti, T. Craddock, R. Courtneidge, M. Zachariadis (eds.), The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries, Wiley, 2020, 86-87.

GEVA B.: Payment Transactions under the E.U. Second Payment Services Directive – An Outsider's View, 54 Tex. Int'l L.J. 211 (2019).

GIROMPINI D.: PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche, in Bancaria, 2018, no.1, 70-73.

GUPTA P.T., THAM M.: Fintech. The New DNA of Financial Services, de Gruyter, 2019.

KOTTAYIL N.M.: Consumer Security and Liability Model for Open Banking, in International Journal of Trend in Research and Development, 2020, 7(4), 230-232.

LEONG E.: Open Banking: The Changing Nature of Regulating Banking Data - A Case Study of Australia and Singapore, in Banking & Finance Law Review, 2020, 35.3, 443-469.

MELI V.: Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento, in M.C. Paglietti, M.I. Vangelisti (eds.), Innovazione e regole nei pagamenti digitali il bilanciamento degli interessi nella PSD2, Roma TrE-Press, 2020, 135-145.

MILANESI D.: A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States, in TTLF Working Papers, 2017, No. 29.

O'DONNELL B.: Data and Privacy in the Next Decade, in King M.R., Nesbitt R.W., The Technological Revolution in Financial Services: How Banks, Fintechs, and Customers Win Together, University of Toronto Press, 2020, 116-128.

PACKIN, N.G.: Show Me the (Data About the) Money!, available at SSRN: https://ssrn.com/abstract=3620025 (forthcoming in Utah Law Review).

PERNG B.J.: Align Open Banking and Future-Proof RegTech for Regulators and Third-Party Providers to Deliver the Optimal Consumer Convenience and Protection, in Barberis J., Arner D.W., Buckley R.P. (eds.), The RegTech Book, he Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation, Wiley, 2019, 89-92.

RAJARETNAM T., YOUNG A.: The promise of an open data economy in Australia: legislating open banking, in Computer and Telecommunications Law Review, 2020, 26(4), 83-90.

REGNARD-WEINRABE B., FINLAYSON-BROWN J.: Adapting to a changing payments landscape, in J. Madir (ed.), FinTech. Law and Regulation, Edward Elgar, 2019, 22-48.
ROTENBERG M.: Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection, in European Law Journal, 2000, vol. 26, 1-2, 141-152
STIEFMUELLER C.M.; Open Banking and PSD 2: The Promise of Transforming Banking by 'Empowering Customers', in Spohrer J., Leitner C. (eds.), Advances in the Human Side of Service Engineering. AHFE 2020. Advances in Intelligent Systems and Computing, vol 1208. Springer, 2020, 299-305.
WOLTERS, P.T.J., JACOBS, B.P.F.: The security of access to accounts under the PSD2, in Computer Law & Security Review, 2019, 35, 29-41.
ZACHARIADIS M.: How 'Open' is the Future of Banking? Data-Sharing and Open Data Frameworks in Financial Services, in King M.R., Nesbitt R.W. (eds.), The Technological Revolution in Financial Services: How Banks, Fintechs, and Customers Win Together, University of Toronto Press, 2020, 129-157.
ZETZSCHE D.A., ARNER D.W., BUCKLEY R.P., WEBER R.H.: The Evolution and Future of Data-Driven Finance in the E.U., in Common Market Law Review, 2020, vol. 57, 331-360.

UDK 336.71:004.9]: 339.137
Review paper

OPEN BANKING AND COMPETITION: AN INTRICATE RELATIONSHIP[1]

Alessandro Palmieri, PhD, Associate Professor
University of Siena, Department of Law
Via P.A. Mattioli 10, 53100 Siena, Italy
alessandro.palmieri@unisi.it

Blerina Nazeraj, PhD Candidate
University of Siena, Department of Law
Via P.A. Mattioli 10, 53100 Siena, Italy
blerinanazeraj@yahoo.it

ABSTRACT

Open banking – promoted in the European Union by the access to account rule contained in the Directive (EU) 2015/2366 on payment services in the internal market (PSD2) – is supposed to enhance consumer's welfare and to foster competition. However, many observers are fearful about the negative effects of the entry into the market of the so-called BigTech giants. Unless incumbent banks are able to rise above the technological challenges, the risk is that, in the long run, BigTech firms could dominate the market, by virtue of their great ability to collect data on consumer preferences, and to process them with sophisticated tools, such as Artificial Intelligence and Machine Learning techniques; not to mention the possible benefits arising from the cross-subsidisation. This paper aims at analysing the controversial relationship between open banking and competition. In this framework, many aspects must be clarified, such as the definition of the relevant markets; the identification of the dominant entities; the relationship with the essential facility doctrine. The specific competition problems encountered in the financial sector need to be inscribed in the context of the more general debate around access to data in the digital sphere. The evolving scenario poses a serious challenge to regulators, calling them to strike the right balance between fostering innovation and preserving financial stability. The appraisal intends not only to cover EU law and policy, but also to make a comparison with other legal systems. In this respect, something noteworthy is taking place in the United States where, as of today, consumers' access to financial data sharing has been largely dependent on private-sector efforts. Indeed, Section 1033 of the Dodd-Frank

[1] Whilst the paper reflects the shared views of the authors, they clarify that Alessandro Palmieri authored, in particular, paras 1, 5, and 6, while Blerina Nazeraj authored paras 2, 3 and 4; they jointly wrote the Conclusions.

Wall Street Reform and Consumer Protection Act (passed in the aftermath of the financial crisis of 2008) provides that, subject to rules prescribed by the Bureau of Consumer Financial Protection (CFPB), a consumer financial services provider must make available to a consumer information, in its control or possession, concerning the consumer financial product or service that the consumer obtained from the provider. This provision, which dates back to 2010, has never been implemented. However, on 22 October 2020, the CFBP has announced its intention to regulate open banking, issuing an advanced notice of proposed rulemaking. In light of their investigation, the authors advocate the adaptation of the current strategies to the modified conditions and, in some instances, the creation of novel mechanisms, more suitable to face unprecedented threats.

***Keywords**: open banking, competition, payment services, innovation, access to data, comparative law*

1. INTRODUCTION

Although several definitions have been proposed[2], as a first approximation, open banking – or, as someone has suggested to rename it, consumer-directed finance[3] – focuses on the ability of banking customers to allow third-party providers to access their bank account data for several purposes. Open banking, which is currently at the centre of a worldwide debate, can be inscribed in the so-called financialization process[4], whose development is supposed to enhance competition in credit markets, especially in the area of payment services and for the benefit of consumers and small and medium-sized firms. In this scenario, incumbent banks are expected to face the challenges posed by genuine FinTech operators, as well as those coming from the area of BigTech companies. The term BigTech is used to refer to the major technology companies with established presence in the market for digital services, whose presence has enormously grown in the financial sector

---

2 For instance, according to the Open Banking Implementation Entity (that was created by the UK's Competition and Markets Authority to prepare software standards and industry guidelines susceptible of driving competition and innovation in UK retail banking), the main feature of open banking is that it "opens the way to new products and services that could help customers and small to medium-sized businesses get a better deal" [https://www.openbanking.org.uk/customers/what-is-open-banking/], Accessed 18 June 2021). On their side, Gupta, P.; Tham, T.M., *Fintech. The New DNA of Financial Services,* de Gruyter, Boston-Berlin, 2019, p. 157, focus on the «adoption of common standards for collaboration between banks and other players within the banking ecosystem».

3 This term was proposed in Canada by the Advisory Committee on Open Banking, appointed by the Minister of Finance in 2018 (see the report titled "*Consumer-directed finance: the future of financial services*", [https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html], Accessed 18 June 2021).

4 The financialization process is characterized by the fact that "change is driven through complementarities and cohesion among supportive regulations, market forces and technological change, whereby new practices and arrangements emerge" (see Gozman, D.; Hedman, J.; Olsen, K.S., *Open Banking: Emergent Roles, Risks & Opportunities*, in AISel Research Papers, 2018, No. 183, p. 3).

in the last few years. Undertakings belonging to the said group would have the capacity to put more pressure on incumbent banks. Indeed, according to a member of the Executive Board of the European Central Bank, "if big tech can speed up loan application processing, reduce transaction costs and improve credit risk assessments, it could increase the overall degree of competition in credit markets"[5]. Yet the coin has another side. The very fact of the entry of tech giants into the market for payment services can be seen not only as something that improves efficiency, but also as an element that threatens to create a new kind of dominance if the market is incapable of correcting[6]. In the following paragraphs, after having outlined the pros and cons of the open banking movement, putting a special focus on BigTechs, we are going to illustrate some of the strategies developed in different geographical areas to deal with this phenomenon.

2. THE BENEFITS AND POTENTIAL DRAWBACKS OF THE EU APPROACH TO OPEN BANKING

Not many authors dealing with the European Union way of promoting open banking, based on the access to account rule contained in the Directive (EU) 2015/2366 on payment services in the internal market (PSD2), have tried to assess its repercussions on competition[7]. However, a common feature of these contributions is that the focus shall be put on the so-called access to account (XS2A) rule, set out in various provisions of PSD2. To this extent, one has to recall, at first, two general provisions concerning the access to payment systems[8] and to the

---

5 Mersch, Y., *Lending and payment systems in upheaval - the fintech challenge,* speech given at the 3rd annual Conference on Fintech and Digital Innovation, Brussels, 26 February 2019 [https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190226~d98d307ad4.en.html], Accessed 18 June 2021.

6 According to Bilotta, N.; Romano, S., *Tech Giants in Banking: The Implications of a New Market Power*, IAI Research Papers, 2019, No. 13, p. 12, at the moment, it is uncertain "whether Techfins do in fact improve competition and efficiency in the banking market, leveraging on better products or services, or whether they actually create concentration powers, using their data superiority and networks effects to create new barriers within the industry".

7 Among the writings on this subject, see Borgogno, O.; Colangelo, G., *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, in *European Business Law Review*, 2020, 31, no. 4, pp. 573-610; Borgogno, O.; Colangelo, G., *The data sharing paradox: BigTechs in finance*, [https://ssrn.com/abstract=3591205], Accessed 18 June 2021; Di Porto, F.; Ghidini, G., *"I Access Your Data, You Access Mine": Requiring Data Reciprocity in Payment Services*, in *International Review of Intellectual Property and Competition Law - IIC*, 2020, 51, pp. 307-329.
On the pros and cons of the UK Open Banking plan, see Borgogno, O.; Colangelo, G., *Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking*, [https://ssrn.com/abstract=3513514], Accessed 18 June 2021 (a revised version is forthcoming in *Journal of European Consumer and Market Law*).

8 Directive (EU) 2015/2366 of the European Parliament and of the Council, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation

accounts maintained with a credit institution[9], and then other two provisions, devoted to specific services, namely to payment initiation services[10] and to account information services[11].

As it has been clearly pointed out in the relevant literature, the XS2A rule shall be considered as "a key factor to strengthen competition in the retail financial markets"[12]. No doubt that this was an important goal of the EU legislative action and, in order to pursue it, it is necessary to enable third parties to obtain access to the customer's payment accounts. Such an access, lowering entry barriers to new players, is a pre-requirement to compete on an equal basis with well-established credit institutions. Of course, the XS2A, and similar rules enacted outside the EU, need to be carefully managed by regulation authorities, which on their side look favourably on tools susceptible of increasing transparency and reducing information asymmetries.

The access to account rule is supposed to include financial technology entities into the relevant market, given their capacity to foster competition through innovation. The digital progress has transformed the traditional banking and financial sector, by allowing new competitors to provide innovative products and services based on consumers' expectations and needs. Such development relies on the availability of customers' bank account data and their processing, crucial for FinTech players' success. Established banks have accumulated that information thanks to their relationship with customers and may refuse to cooperate with market entrants because of the risk of losing control over their customers and being marginalized[13]. Art. 36 of PSD2 aims at avoiding foreclosure practices by granting real-time access to customer's account data for authorized payment services providers and thus reducing informational barriers to entry. This could result in an enhancement of consumers' welfare. As a matter of fact, the so-called front-end providers act as intermediaries between the customers (payees and payers) and the account servicing payment service providers (ASPSPs), such as banks, making transactions easier[14].

(EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35 (PSD2), art. 35.

9 PSD2, art. 36.

10 PSD2, art. 66.

11 PSD2, art. 67.

12 Borgogno, O.; Colangelo, G., *Data, Innovation …*, *op. cit.*, note 7, p. 575.

13 According to Borgogno, O.; Colangelo, G., *Data, Innovation …*, *op. cit.*, note 7, p. 585, "Under the PSD, banks could legitimately refuse to grant any access or to share sensitive information with TPPs due to intellectual property and security issues as well as to reputation risks and for liability reasons. In the same vein, customers who shared their account security information breached their contract with the bank exposing themselves to major consequences".

14 Borgogno, O.; Colangelo, G., *Data, Innovation …*, *op. cit.*, note 7, p. 579, distinguish these entities from end-to-end providers, which "are closed platforms that interact both with the payer and payee

In particular, payment initiation services providers (PISPs) initiate payments on the customer's behalf from her or his bank account and inform the payee that the funds' transfer was made; while account information services providers (AISPs) manage the information from multiple customer accounts, aggregating them so that the user can get an overall view of her or his financial position[15]. According to art. 67 of PSD2, this kind of FinTech provider can access both the information from designated payment accounts and associated payment transactions.

Nonetheless, the writings on this subject are not limited to emphasizing the hypothetical advantages of the Open banking revolution. The regulatory choices made by the EU legislator when enacting the XS2A rule have been highly criticized for various reasons. One of the authors has directed his criticism more particularly against the excessive attention given to concerns about the competitiveness of the business environment, which is likely to overshadow other values worthy of protection, such as consumers' interests and data protection[16]. In our opinion, the said values must be taken into account by those who are involved in the open banking movement, in the sense that a proper balance has to be found (and maintained) between the interests at stake. With respect to privacy concerns, one cannot deny that the XS2A rule is the cornerstone of one of the specific data access regimes created by EU legislation. Although these regimes aim at promoting objectives beyond the protection of personal data, they are necessarily to be coordinated with the general principles that grant to the data subject a strong control over her or his personal data[17].

Other commentators, although inclined to think that the provisions enacted at the EU level might boost competition in the consumer retail payments market, are fearful that the current efforts are not enough to undermine the hegemonic position of the largest banks. Path dependence plays a role here, preventing or slowing down fully optimal adjustments. A recent study has shown that, if con-

---

arranging transactions within their system".

15 See Vezzoso, S., *Fintech, access to data, and the role of competition policy*, in Bagnoli, V. (ed.), *Competition and Innovation*, Scortecci, São Paulo, 2018, p. 32.

16 This is the view expressed by Stiefmueller, C.M., *Open Banking and PSD 2: The Promise of Transforming Banking by 'Empowering Customers'*, in Spohrer, J.; Leitner C. (eds.), *Advances in the Human Side of Service Engineering. AHFE 2020. Advances in Intelligent Systems and Computing*, vol. 1208, Springer, Cham, 2020, pp. 299-305.

17 According to Graef, I.; Husovec, M.; van den Boom, J., *Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, in *Journal of European Consumer and Market Law*, 2020, 9(1), pp. 3-16, in the EU the sector-specific data access regimes are internal market-focused. On its side, "GDPR can be regarded as a regime that sets the boundaries within which sector-specific data access regimes can regulate other objectives that inevitably relate to the processing of personal data" (p. 6).

sumers are asked to share their payments data, only a minority of them "would give consent to other banks they are not customers of or to newcomers in the payments market"[18].

3. THE ROLE OF BIGTECH PLAYERS

Assuming that the ongoing processes are successful in mitigating the problems deriving from the alleged hegemony of Big Banks, other risks are looming on the horizon. Indeed, established financial institutions will have to deal not only with emerging business entities, exclusively or mainly focused on the banking and financial industry, but also with the so-called BigTechs. In general terms, it is undeniable that FinTech firms, primarily those which provide services in the B2C segment, can act as credible challengers to traditional organisations[19]. This is precisely the goal, or at any rate one of the goals, that decision-makers and regulators hope to achieve[20].

Nevertheless, as we mentioned above, financial institutions will suffer – in fact, they are nowadays suffering – an attack from BigTech companies. The advantages and disadvantages of the entry of these firms into the retail payments market have already been identified. Contrary to what it may seem at a first glance, the descent into the field of BigTech players may be counterproductive for competition[21]. On the one hand, such companies might amplify the effects of FinTech disruptive impact; on the other hand, as it has been highlighted in a Report released by a leading international management consulting firm (Oliver Wyman) and the Inter-

---

18 See Bijlsma, M.; van der Cruijsen, C.; Jonkera, N. *Consumer willingness to share payments data: trust for sale?*, TILEC Discussion Paper, 2020-015. The authors argue that: "Newcomers need to work on gaining people's trust, and show that their payments data is safe with them. Furthermore, they may attract customers by offering them financially attractive products, as consumers' demand for PSD2 services turns out to be sensitive to prices. They might be able to do so, in product markets where the margins are high and by making intelligent use of people's payments data so that they can make tailor made offers, which adequately price credit risks" (p. 19).

19 It is virtually unanimously acknowledged that FinTech "has become such a disruptive force in such a short time period that established financial institutions must quickly reconsider their business model" (see, for instance, Assay, B.E., *FinTech for Digital Financial Services: The African Case*, in Rafay, A., *FinTech as a Disruptive Technology for Financial Institutions*, IGI Global, Hershey, PA, 2019, p. 67).

20 According to Gozman, D.; Hedman, J.; Olsen, K.S., *Open Banking: Emergent Roles …*, *op. cit.*, note 4, p. 5, "today's fintech movement and provisions for access-to-accounts are partly being driven by regulators keen to accelerate the competition and digital disruption that is reshaping the financial services industry and also to further increase transparency and reduce information asymmetries".

21 De la Mano M.; Padilla, J. *Big Tech Banking*, in *Journal of Competition Law and Economics*, 2018, 14(4), pp. 494-526, argued that, although the entry of BigTech companies into the market could enhance competition in the short term, there is a significant risk that this will result in more concentrated credit markets in the long term.

national Banking Federation, BigTechs differs from FinTechs in several ways[22]. It is not just a quantitative matter. In the said Report, the divergences are analysed. Probably the most important of all is that BigTech companies, when deciding a certain financial service, aim at "monetizing existing core businesses and serving customers holistically than the financial service itself"[23].

Some authors predict that, relying on their great ability to collect data on consumer preferences, and to process them with sophisticated tools, such as Artificial Intelligence and Machine Learning techniques, in the near future BigTech companies will be able to dominate at least some segments of the retail banking industry[24]. This could happen regardless of whether these companies will act as intermediaries or marketplaces[25]. Of course, large banks make use of Artificial Intelligence. But BigTech companies may combine Artificial Intelligence with the ability to collect and process big data. This phenomenon has already attracted attention from competition authorities: one can simply recall the decision regarding Facebook's processing of users' data issued in 2019 by the Bundeskartellamt; and the investigations recently launched against the same platform by the European Commission and the UK Competition and Markets Authority.

Taking into account these factors, scholars usually criticize the EU approach because it does not really level the playing field, and it underestimates large technology companies' impact. The XS2A rule might prove to be disproportionate, given that it does not consider the differences between FinTech and BigTech entrants. We can take for granted that the advent of FinTech companies will be beneficial to the whole system: they can exploit efficient technologies without being burdened by legacy systems; they do not enjoy significant financial resources, an established

---

22 The joint report, published in 2020, is titled, *Big Banks, Bigger Techs?*, and is available on the website www.oliverwyman.com.

23 *Big Banks, Bigger Techs?*, *op. cit.*, note 22, p.16.

24 See Padilla, J., *BigTech "banks", financial stability and regulation*, in *Estabilidad financiera*, 2020, issue 38, pp. 11-26; in particular, the phenomenon is expected to occur in the area of distribution of loans to consumers and SMEs (p. 14).

25 According to Padilla, J., *BigTech "banks"…*, *op. cit.*, note 24 p. 14-15, "BigTech platforms may enter as "intermediaries", in direct competition with incumbents, raising funds and lending them to consumers and firms, or as "marketplaces", offering customers the ability to engage with many financial institutions (banks and non-banks) using a single distribution channel. As intermediaries, they may be able to offer new services by bundling their existing offerings (e.g. online advertising, e-commerce, etc.) with traditional banking products; e.g. offering cheap credit to customers who subscribe to their online services or purchases in their e-commerce sites. […]. As marketplaces, they may benefit from network effects by bringing together banks. and borrowers. Banks may need join these platforms in order to reach out to borrowers. Borrowers will patronize them to obtain cheaper credit. Each of these marketplaces likely will auction the loans it originates amongst all, or at very least a significant fraction, of the banks participating in its platform".

customer base, a reputation and brand recognition; and, like banks, they are characterized by limited skills in managing big data analytics. From this point of view, the right to access will likely increase competition and contestability of banking markets as well as consumer welfare in terms of diversified products and services, lower transaction costs, and price reduction.

However, in the long term, the access to account rule may lead to monopolization by BigTech companies[26], which enjoy scale and scope economies, an established-loyal customer base, a vast amount of digital customer data, a solid reputation, and strong brands. Furthermore, they can collect information about consumers' behaviour from nonfinancial activities, such as research and social media and analyse them with artificial intelligence or cloud computing techniques to offer new and tailored services. Large Tech entities, when dominant, may engage in anti-competitive practices by bundling their services with banking products, discriminating incumbents in favour of their affiliates within their platforms, as well as privileging their own products and services. The latter strategy stands out mainly when they act both as an intermediary and a business operator[27]. Within this framework, traditional banks may suffer a competitive disadvantage, given that they gather only financial data and have to deal with rigid regulation and legacy technologies. The XS2A rule may distort competition by obliging them to share with big digital providers the only advantage they hold (customers' account data) without something in return.

In this regard, some commentators suggest the introduction of a "reciprocity clause" that should grant credit institutions access to the data owned by the beneficiary of the XS2A rule if this is a tech giant[28]. This solution may enable banks to

---

[26] According to the Organisation for Economic Co-operation and Development (OECD), *Digital Disruption in Banking and its Impact on Competition*, 2020 [http://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm], Accessed 18 June 2021), "FinTech will certainly increase the contestability of banking markets and increase competition in the short term. Whether the entry of BigTech platforms will entrench large players with dominant positions, and whether it may raise systemic risk concerns, is unknown".

[27] Borgogno, O.; Colangelo, G., *The data sharing paradox …*, *op. cit.*, note 7. See also OECD, *Digital Disruption in Banking and its Impact on Competition*, *op. cit.*, note 26, p. 22, where the potential strategies of incumbents and Big Tech platforms are analysed, pointing out that: "Incumbents have limited options for staying in business if BigTech firms enter the banking sector in full force. Either they can become platforms and compete directly with BigTech firms by trying to compensate for the latter's superior data capabilities, perhaps greater client trust and security (banks are good at keeping secrets), and better ability to navigate the regulatory maze, or they can become specialised in unique financial products that the BigTech firms cannot offer and therefore cannot commoditise. In any case, incumbents will have to restructure, and consolidation will occur".

[28] Among the others, see Di Porto, F.; Ghidini, G., *"I Access Your Data, You Access Mine" …*, *op. cit.*, note 7, p. 323.

exploit both customers' account data and other behavioural information to provide more efficient digital payment services. According to those who support the reciprocity clause (which would need amendments to PSD2[29]), data subject consent represents the legal ground of the reciprocity obligation. In order to clarify the scope of the reciprocity obligation, one has to solve the problem of defining the information to which banks should access as compensation for customers' account data sharing. In this respect, it has been argued that, unlike account information, behavioural data cannot be considered indispensable to provide digital payment services, and BigTech companies do not enjoy monopoly power in their generation and collection[30]. According to the reciprocity clause's supporters, banks should access only the data held by Big Tech platforms which are necessary to provide their own services and are authorized by the data owner, pursuant to art. 66 of PSD2[31].

It is worth noting that the XS2A rule seems to introduce access to an essential facility. Following the essential facility doctrine – and setting aside the complexity of defining it – a dominant company cannot refuse to share its assets if they are fundamental for competitors to provide their products or services[32]. Obviously, this doctrine aims at preventing the monopolist from excluding new entrants. The

---

29 Di Porto, F.; Ghidini, G., *"I Access Your Data, You Access Mine"* …, *op. cit.*, note 7, p. 326, have proposed to integrate art. 66 PSD2 with a new lit. (i), formulated as follows: "(i) the payment initiation service provider with an initial capital of €XXX or above [or with an annual capital equal or above €XXX, or with more than XXX active personal clients] shall, immediately after confirmation by the account servicing payment service provider that its payment order was received, provide or make available to the account servicing payment service provider all information regarding the payment service user in its possession. A similar amendment should be made to Art. 67, with reference to AISPs".

30 Borgogno, O.; Colangelo, G., *The data sharing paradox* …, *op. cit.*, note 7, p. 10.

31 Di Porto, F.; Ghidini, G., *"I Access Your Data, You Access Mine"* …, *op. cit.*, note 7, p. 324. Speaking about big data, OECD, *Big Data: Bringing Competition Policy to the Digital Era, Executive Summary,* April 26, 2017 [https://one.oecd.org/document/DAF/COMP/M(2016)2/ANN4/FINAL/en/pdf], Accessed 18 June 2021, has observed that competition authorities should assess, in each specific case, whether the data are replicable, if they can be obtained in other ways, how much data are needed to compete, in order to consider refusals to give access to data and discriminatory access to them as anti-competitive conducts (p. 4).

32 According to the European Commission, *Staff Working Document on the free flow of data and emerging issues of the European data economy*, January 10, 2017 [https://digital-strategy.ec.europa.eu/en/library/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy], Accessed 18 June 2021, competition authorities can invoke the essential facility doctrine to grant access to data held by an economic operator if the four conditions laid down by the Court of Justice of the European Union are fulfilled. In particular, data should be indispensable for the downstream product, there would not be any effective competition between the upstream and downstream product, the refusal would prevent the development of the second product without an objective justification (p. 21-22). About the essential facility doctrine, see the following judgments of CJEU: Joined Cases C-241/91 P and C-242/91 P *RTE and ITV v Commission* [1995] ECR I-743; Case C-418/01 *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG* [2004] ECR I-5039; Case C-170/13 *Huawei Technologies*

question is whether customers' account data can be considered an essential facility. Before the PSD2, third-party providers were able to collect account information thanks to the practice of screen-scraping, also known as web scraping, which consists in an "automated, programmatic use of software via which the customer allows a third party (such as a FinTech) to extract data or perform actions that users would usually perform manually on the website, by sharing with the latter their security credentials"[33]. This means that the data access at issue was not completely excluded for newcomers. Nowadays, customers' account data cannot be qualified as an essential facility because of the free-of-charge access granted by the XS2A rule and the absence of any agreement between the banks and third-party providers. Moreover, it should not be ignored the difficulty of defining the data relevant market, given the involvement of both antitrust law and specific financial regulation that may lead to conflicting outcomes[34]. The PSD2, indeed, does not attribute specific competences to financial authorities in order to ensure competition in the payment services industry, meaning that competition law is still applicable[35]. Additionally, even if the said limitations can be overcome, the bank's dominant position is a prerequisite that should be verified on a case-by-case basis, preventing the general applying of such an antitrust remedy[36].

Speaking about the existence of a dominant position, it is really questionable whether financial institutions (even those of large dimensions) can be considered hegemonic in the context of a market populated by agents labelled as BigTechs. For the reasons explained above, it is plausible to believe that the balance hangs on the side of these latter entities. Many authors agree on the fact that the access to, and the control of, huge amounts of data (not necessarily personal data[37]) is a source of market power[38]. Indeed, the economic success of digital platforms depends on the number of their users, seen as a data source. The more users there are, the more information can be gathered by these companies and exploited to

---

Co. Ltd v. ZTE Corp. and ZTE Deutschland GmbH ECLI:EU:C:2015:477. See also the judgment of the Court of First Instance in Case T-201/04 *Microsoft Corp. v. Commission* [2007] ECR II-3601.

33 Borgogno, O.; Colangelo, G., *Data, Innovation …*, *op. cit.*, note 7, p. 588.

34 Di Porto, F.; Ghidini, G., *"I Access Your Data, You Access Mine" …*, *op. cit.*, note 7, p. 315.

35 Vandenborre, I.; Levi, S.D.; Janssens C., *Fintech and access to data*, in *Concurrences*, 2019, N° 4, p. 3.

36 Borgogno, O.; Colangelo, G., *Data, Innovation …*, *op. cit.*, note 7, p. 583.

37 With respect to interaction between competition and personal data protection law, see. Paal, B.P., *Market Power in Data (Protection) Law*, in *Global Privacy Law Review*, 2021, vol. 2, issue 1, pp. 8-15; the Author believes that "data protection and antitrust law do not communicate dissonantly, but rather harmoniously" (p. 15).

38 See, for instance, Santesteban, C.; Longpre, S., *How Big Data Confers Market Power to Big Tech: Leveraging the Perspective of Data Science*, in *The Antitrust Bulletin*, 2020, vol. 65, issue 3, pp. 459-485; United Nations Conference on Trade and Development (UNCTAD), *Competition issues in the digital economy*, 2019, p. 6.

increase the quality of the service, also by selling the data at issue to advertisers for tailored advertising. This may represent a barrier to entry for potential entrants that do not enjoy such an opportunity[39]. Similarly to what is happening in other segments of the digital landscape, there is a widespread awareness that online platforms have gained a dominant position in their respective markets[40], or they are on the way to become dominant[41].

From a general point of view, presumably a novel approach must be developed to deal adequately with the competition dilemmas in the platform economy. Or at least, enforcers are called to adapt the existing tools [42]; and, of course, this adaptation could take place in different forms[43]. In any case, an adjustment of the current strategies, or sometimes the creation of new paradigms, seems inevitable, and we think that it is urgent too (although the performance of these tasks requires some time). These processes may lead to various outcomes, even unexpected ones. But the end result cannot reasonably be that the platform competing with banks in the retail payments market is always regarded as the dominant entity that, facing a number of small competitors, acts like a monopolist. One of the risks is that of

---

39 UNCTAD, *Competition issues in the digital economy*, *op. cit.*, note 38, p. 4.

40 See Hermes, S.; Pfab, S.; Hein, A.; Weking, J.; Böhm, M.; Krcmar, H., *Digital Platforms and Market Dominance: Insights from a Systematic Literature Review and Avenues for Future Research*, PACIS 2020 Proceedings, 42.

41 Such risks are perceived all over the world. In China, the State Administration for Market Regulation issued (on February 7, 2021) the Platform Antimonopoly Guidelines, with the aim of preventing and stopping monopolistic behaviour in the platform economy. In Germany, the 10th amendment to the German Competition Act – which has entered into force on January 19, 2021 – focuses on the platform economy; according to the President of the German Competition Authority (Bundeskartellamt), the reform will permit "to prohibit big tech companies from engaging in certain types of conduct much earlier and, so to speak, shut the stable door before the horse has bolted" (the press release published by the Bundeskartellamt is available at [https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/19_01_2021_GWB%20Novelle.html], Accessed 18 June 2021).

42 UNCTAD, *Competition issues in the digital economy*, *op. cit.*, note 38, p. 5, has expressed the view that "competition law and policy […] need to be adapted to the new market realities and business models. This is crucial to ensure competitive and contestable markets".

43 Sitaraman, G., *Too Big to Prevail: The National Security Case for Breaking up Big Tech*, 99 Foreign Aff. 116 (2020), pushes for breaking up BigTech companies. According to Hovenkamp, H.J., *Antitrust and Platform Monopoly*, U of Penn, Inst for Law & Econ, Research Paper No. 20-43 (forthcoming in 130 Yale L.J. (2021)): "Competition problems in digital platforms present some novel challenges, but most are within reach of existing antitrust law's capacity to handle them. The courts and other antitrust policy makers should treat digital platforms for what they are, which is business firms that have unique features but not very much that requires us to abandon what we know about competition in high-technology, product-differentiated markets" (p. 121).

defining markets too narrowly[44], and thus ignoring the competitive pressure of other firms.

We firmly believe that, in the absence of a profound renovation of the antitrust conceptual framework, further regulatory measures are required. And, in order to find an efficient solution, further research is needed to fully understand the mechanisms that govern the interaction between platforms and other market agents.

4. OTHER CRITICAL ISSUES REGARDING DATA SECURITY IN DIGITAL PAYMENTS

Since data are the main asset of online banking, there is a risk of illegitimate use and access to customer information. The client trust is a key prerequisite for the provision of digital payment services, given that without his or her consent there is no data flow. In order to ensure the confidentiality and integrity of customer data, the PSD2 prevents the PISP from accessing, using, or storing any data that are not necessary for the provision of the payment service requested by the payer. The bank shall give access to all the available data about the customer's account unless they are deemed sensitive. The PISP cannot share the user's security credentials with parties other than the user himself and the bank. Third-party providers must also identify themselves towards the credit institution and communicate with the latter, the payer, and the payee in a secure manner[45]. Furthermore, PISPs are expected to take appropriate measures to deal with operational or security incidents[46]. Finally, the PSD2 mandates PISPs to implement Strong Customer Authentication (SCA) processes, complying with the technical requirements developed by the European Bank Authority (EBA) in cooperation with the European Central Bank and approved by the European Commission[47]. The Regulatory Technical Standards regulate both the identification of providers and user authentication. The enhanced authentication is based on three elements, such as something only the customer knows (password/PIN), something only the user possesses (smartphone/device) and something inherent to the user (fingerprint/facial recognition)[48].

---

44 On this issue, with specific reference to two-sided platforms, see Franck, J-U.; Peitz, M., *Market Definition in the Platform Economy*, CRC TR 224 Discussion Paper Series, 2021; Sarmas, I., *Market Definition for Two-Sided Platforms: Why Ohio v. American Express Co. Matters for the Big Tech*, 19 Fla. St. U. Bus. Rev. 199 (2020).

45 PSD2, art. 66.

46 PSD2, art. 96.

47 The PSD2 (articles 95, 96 and 98) has mandated the EBA to develop guidelines and drafts of Regulatory Technical Standards to ensure data security and implementation of the XS2A rule.

48 PSD2, art. 4.

The EBA prevents third-party providers from accessing customer data through screen-scraping, thus avoiding fraud and data abuse risks[49]. The screen-scraping mechanism is not considered secure[50]. Instead of this mechanism, the Authority endorses the use of application programming interfaces (APIs), which are sets of protocols that allow communication between computer applications (interfaces). They facilitate the connection between account providers, their customers and payment services providers, making accessible, unlike screen-scraping, only the payment information that the interface allows. Management of APIs is crucial for the effective enforcement of the access to account rule. The discussion among market players and policymakers focuses on whether standardize APIs or let ASPSPs free to exploit their own interfaces[51]. The European Parliament opted for the standardization strategy in line with the aim of harmonization and interoperability[52]. Additionally, the EBA has set up a Working Group on APIs to address their opportunities and challenges.

With respect to the relationship between PSD2 and data protection law, art. 4 of the General Data Protection Regulation (GDPR)[53] defines account data as personal data. Art. 94 of PSD2 states that payment service providers can access, process, and retain the personal data necessary to provide their payment services, with the payment service user's consent. But most important, art. 20 of GDPR grants the right to data portability, according to which the data owner has both the right to receive the personal data he or she has provided to a controller and the right

---

49 See European Banking Authority, *Opinion of the European Banking Authority on the European Commission's intention to partially endorse and amend the EBA's final draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2,* June 29, 2017: "Current access approaches, often referred to as 'screen scraping', in which the TPP impersonates the consumer and has access to all the consumer's data, rather than only the data necessary to provide payment services, would not be compliant".

50 See Zunzunegui, F., *Digitalisation of Payment Services*, Ibero-American Institute for Law and Finance, Working Paper Series, No. 5/2018, p. 26: "Since the passwords are assigned, all of the customer's data can be Accessed without any restrictions, except for the protections that the bank itself may develop for this kind of access".

51 Borgogno, O.; Colangelo, G., *Data, Innovation …*, *op. cit.*, note 7, p. 591, analyse the pros and cons of the APIs standardization. For instance, in the United Kingdom the main credit institutions has been mandated by the Competition and Market Authority to design "a single a single, open standardized set of APIs freely available for the whole industry". See also Borgogno, O.; Colangelo, G., *Data Sharing and Interoperability Through APIs: Insights from European Regulatory Strategy*, in *Computer Law & Security Review*, 2019, vol. 35, issue 5.

52 European Parliament, *FinTech: the influence of technology on the future of the financial sector*, May 17, 2017 [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0211_EN.html], Accessed 18 June 2021.

53 Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR).

to transmit those data to another controller. It is necessary to coordinate art. 20 GDPR with the XS2A rule, given that the bank customer could migrate his or her data from the traditional bank to the FinTech company relying on the right to data portability. The matter was solved by the EU "Working Party Article 29" using the *lex specialis* criterion, according to which the PSD2 shall prevail, given its sectorial regime[54]. Further details on this issue have been provided by the European Data Protection Board (EDPB) – the successor of the said Working Party – in the Guidelines on the interplay of PSD2 and the GDPR, adopted on 17 July 2020[55]. It has been clarified that the notion of "explicit consent" under the PSD2 is different from (explicit) consent under the GDPR. Indeed, the first one is an additional requirement of a contractual nature.

5. A LOOK AT THE STRATEGIES DEVELOPED IN THE GLOBAL FRAMEWORK

Attempts to regulate open banking are carried out in several geographical areas, in order to stimulate the competitiveness in the payments market and to avoid the creation of new, and potentially more dangerous, forms of distortions. Trespassing the borders of the European Union, we immediately encounter the United Kingdom, whose experience had its roots in the EU legislation, but then partially deviated from the common track.

Australia has implemented an open banking system, in a larger framework of promotion of the sharing of data among firms. Actually, in July 2020, the Australian Consumer Data Right Act came into force, which pursues the goal of improving competition and choice, as allows that transaction data, customer data and product data can be communicated with third-party comparison sites to increase the consumer's negotiation strength. The scope of this piece of legislation is overly broad: in the initial stage, it is applicable only in the banking industry; then it will apply to the energy and telecommunications sectors, before including other industries gradually on a sector-by-sector basis.

Speaking of recent developments, one cannot ignore how Brazil is coping with open banking. In May 2000, the Central Bank of Brazil (Banco Central do Brasil) has issued a regulation on the implementation of open banking. Like similar attempts to govern the phenomenon, the said regulation – which defines open banking as a standardized sharing of data and services through the opening and

[54] See Art. 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*.

[55] EDPB, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR.

integration of systems – aims at encouraging innovation, promoting competition, and increasing the efficiency of the national financial system.

Of particular interest is the case of Canada, where in June 2019, the Senate Committee on Banking, Trade and Commerce asked the Government to take immediate steps to initiate an open banking framework. Then, in January 2020, the Advisory Committee on Open Banking, appointed by the Ministry of Finance, determined that the benefits of open banking outweigh its cost. In its report[56], the Committee observed that a robust consumer-directed framework: *i*) could give consumers greater control of their information; *ii*) could support a more innovative and competitive sector by setting rules and protections around data use and requiring data to be transferred in a more secure form. After the publication of this report, a new phase commenced in the design of an open banking regulatory framework. Currently, the focus is on determining how regulators and the financial sector can mitigate data security and privacy risks.

6. THE UNITED STATES EXPERIENCE: REGULATION IS NEEDED?

It is really remarkable what is currently taking place in the United States. Unquestionably, in this field, the United States have adopted for many years a laissez-faire strategy. Consequently, the developments have been market-driven[57]. However, some factors, and in the first place the unwillingness of many banks to provide third-party companies with access to customer accounts, delay the expansion of open banking in the United States[58].

But significant changes might occur soon. Recently, the Bureau of Consumer Financial Protection (CFPB) – a federal agency created under the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) with the purpose to promote fairness and transparency for mortgages, credit cards, and other consumer financial products and services – made a move could be a bellwether for a potentially radical turn in the approach to the problem under discussion. The Dodd-Frank Act, enacted in response to the global crash of 2008, contained several measures aimed at preventing financial crises. What is relevant

---

56 *Consumer-directed finance …*, *op. cit.*, note 3.

57 See Kaufman Winn, J.; Wright, B., *The Law of Electronic Commerce*, 4th ed., Wolters Kluwer, New York, NY, 2021, § 7.09[B].

58 In this respect, Liu, H.-W., *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and its Open Banking Watershed Moment*, 30 Wash. Int'l L.J. 28, 31 (2020), has observed that, in comparison to the European situation. "the financial data-sharing environment is less clear in the United States, which lags in building up Open Banking".

to our purposes is that there is a provision (section 1033) titled "Consumer rights to access information". This provision obliges consumer financial services provider to make available to a consumer, upon request, information in its control or possession concerning the consumer financial product or service that the consumer obtained from the said provider, including information relating to any transaction, series of transactions, or to the account, such as costs, charges, and usage data. It is specified that this information shall be made available in an electronic form usable by consumers.

The implementation of the statutory measures requires the promulgation of specific regulation by the CFPB. For about ten years the Bureau, although backing up in some way consumers' interest in access to (and control of) financial data[59], has not taken any step to put into effect the provisions. Finally, after the organization in February 2020 of a "Symposium on Consumer Access to Financial Records and Section 1033 of the Dodd-Frank Act", the CFPB issued, on October 22, 2020, an Advance Notice of Proposed Rulemaking (ANPR) to solicit comments and information to assist the Bureau in developing the necessary regulations[60].

The document underlines that "consumer-authorized data access and use holds the promise of improved and innovative consumer financial products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services to consumers". Then it aims at showing the positive effect, in terms of intensification of competition, of the implementation of the rule about consumer right to access information. More specifically, the ANPR supports the view that authorized data access is susceptible not only of fostering competition for existing products (which could be accessed by a larger number of customers, and at a lower price), but also of stimulating the offer of new types of products and services. Moreover, consumers are expected to gain also from the improvement of existing products.

The endeavour of the CFPB to create a congenial environment does not mean that the private sector will fade into the background. On the contrary, since private

[59] Among the initiatives promoted by the Bureau, before taking its fundamental step, Vallabhaneni, P., *CFPB Seeks Comments on Highly Anticipated Consumer Access to Financial Information Rulemaking* (Nov. 3, 2020), [https://www.whitecase.com/publications/alert/cfpb-seeks-comments-highly-anticipated-consumer-access-financial-information], Accessed 18 June 2021, recalls the "principles for Consumer-Authorized Financial Data Sharing and Aggregation covering access; data scope and usability; control and informed consent; authorizing payments; security; access transparency; accuracy; ability to dispute and resolve unauthorized access; and efficient and effective accountability mechanisms".

[60] 85 FR 71003.

sector initiatives are driving the adoption of open banking in the United States[61], it is advisable that the strategies pursued by the Bureau will be coordinated with those of financial institutions and technology companies.

The ANPR aroused many reactions. As far as we know, 99 comments have been submitted on the dedicated webpage, where they are accessible[62]. Remarkably interesting are the observations of the American Bankers Association, especially where the comment emphasizes the risk of implementing prescriptive standards, which may undermine the progress that has already taken place. The fear is that standards, which in their essence are static, are going to create obstacles to innovation[63]. In our view, since common standards facilitate the entry into the market by non-incumbent financial services providers, a flexible approach would be recommended, fostering market standards that are capable of accommodating innovation[64]. For instance, one could think of a single platform that allows applications to interoperate with distinct cloud providers' services using a normalized interface[65].

---

61 According to a report prepared for the Federal Reserve Bank of Boston (Pandy, S., *Modernizing U.S. Financial Services with Open Banking and APIs* (Feb. 8, 2021) [https://www.bostonfed.org/publications/payment-strategies/modernizing-us-financial-services-with-open-banking-and-apis.aspx], Accessed 18 June 2021), three initiatives are noteworthy: 1) the creation of a Model Data Access Agreement, prepared by The Clearing House, a company owned by 24 of largest United States leading commercial banks, for which it provides payment, clearing, and settlement services; 2) the generation, in the market for consumer and small business financial services, of several frameworks directed to develop common standards for open banking; 3) the acquisition, by some companies operating in the said market, of data aggregators, which serve as central hubs for sharing bank account data with all the applications that need it.

62 The comments are available at [https://www.regulations.gov/document/CFPB-2020-0034-0001/comment], Accessed 18 June 2021.

63 On this point, see also Competition Bureau Canada, *Supporting a competitive and innovative open banking system in Canada* (Jan. 18, 2021), [https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04571.html], Accessed 18 June 2021: "a Common Standard can negatively impact innovation and dynamic competition when new standards arise. Common Standards are by definition rigid, and deviation from these standards, even in circumstances where there may be value in doing so, could require a number of bi-lateral agreements between financial service providers to act outside of the pre-determined Common Standard. This creates a lack of flexibility that can reduce the incentives for service providers to bring about innovative ways of exchanging data, to the detriment of dynamic competition" (§ 18).

64 In this line of thinking, see Competition Bureau Canada, *Supporting a competitive and innovative open banking system*, *op. cit.*, note 63, § 19.

65 See L.A. Bastião Silva, C. Costa, J.L. Oliveira, *A common API for delivering services over multi-vendor cloud resources*, in *Journal of Systems and Software*, 2013, vol. 86, issue 9, 2309-2317.

7. CONCLUSION

The Canadian Competition Authority noted that open banking is not automatically pro-competitive; the achievement of a satisfactory result "requires careful design and ongoing regulatory support. Accordingly, decision makers must actively ensure that regulatory rules are successful in achieving their intended policy goals"[66]. We agree with this point. As outlined above, the rise of open banking brings serious concerns for competition. These concerns must be addressed, not by creating rigid barriers for BigTechs (since, to a certain extent, their contribution could be beneficial to improve consumer welfare)[67], but regulating in a proper manner the coexistence between traditional financial institutions, 'ordinary' FinTech companies, and BigTech giants. In the absence of a specific regulatory treatment of BigTechs operating in finance[68], a new model of regulation should be adopted[69]. We are not worried about the emergence of new forms of competition in the banking and financial sector. And, as it should be clear from the above paragraphs, our purpose is not to defend the established hierarchies and structures. But we fear, in tune with other authors' way of thinking, that, unless the process is carefully controlled by legislatures and regulators, that online platforms will replace the hegemony of the traditional banks.

In this scenario, competition law should play a non-secondary role, especially when problems are specific to single firms[70]. And the answer to the failures of traditional antitrust enforcement to face digital gigantism cannot simply be the

---

66 See Competition Bureau Canada, *Supporting a competitive and innovative open banking system*, *op. cit.*, note 63, § 9.

67 According to Borgogno, O.; Colangelo, G., *The data sharing paradox …*, *op. cit.*, note 7, p. 13, since "FinTech start-ups seem more likely to work alongside incumbent banks rather than compete with them, imposing entry barriers to BigTechs would remove the only effective source of competitive pressure for traditional banks".

68 See Crisanto, J.C.; Ehrentraud, J.; Fabian, M., *Big techs in finance: regulatory approaches and policy options*, FSI Briefs, 2021, No. 12, p. 8.

69 According to Crisanto, J.C.; Ehrentraud, J.; Fabian, M., *Big techs in finance …*, *op. cit.*, note 7, p. 12: "The entry of big techs into finance calls for a comprehensive public policy approach that combines financial regulation, competition policy and data privacy. Policy options that could be considered include adjusting the existing policy approach by recalibrating the mix of entity-based and activity-based rules, in favour of the former in certain policy areas; developing a bespoke regime for big techs; and strengthening cross-sectoral and cross-border cooperative arrangements between national authorities and foreign regulators. These options may support authorities in their considerations on how best to adjust the regulatory framework in their efforts to address the risks that the business model of big techs entails while preserving the benefits they create".

70 See Hovenkamp, H.J., *Antitrust and Platform Monopoly*, *op. cit.*, note 43, p. 120: "Antitrust's fact-specific, individual approach to intervention is superior to regulation when failures of competition are specific to the firm rather than inherent in the market". On their side, Borgogno, O.; Colangelo, G., *The data sharing paradox …*, *op. cit.*, note 7, p. 13, observe that "there will always be room for antitrust

re-proposition of the idea that 'big is bad', at the expense of consumer welfare[71]. Authorities and other decision-makers need to be extremely cautious when enacting restrictive measures, since over-regulating platforms involved in the provisions of payment services could be counterproductive. Looking specifically at the European context, EU institutions, to achieve a better result, should also analyse carefully what is going on in other geographical areas. Indeed, the establishment of an effective dialogue among the agencies that – in different (national as well as supranational) legal systems – are responsible for the sectors connected with consumer-directed finance (such as banking authorities, financial market authorities, competition authorities, data protection authorities) seems necessary to tackle a global problem. This might seem obvious, but experience has shown that synergy among the different authorities is quite difficult to achieve. So legislative measures are needed to incentivize cooperation.

REFERENCES

BOOKS AND ARTICLES

1. Assay, B.E., *FinTech for Digital Financial Services: The African Case*, in Rafay, A., *FinTech as a Disruptive Technology for Financial Institutions*, IGI Global, Hershey, PA, 2019, p. 67.
2. Bijlsma, M.; van der Cruijsen, C.; Jonkera, N. *Consumer willingness to share payments data: trust for sale?*, TILEC Discussion Paper, 2020-015.
3. Bilotta, N.; Romano, S., *Tech Giants in Banking: The Implications of a New Market Power*, IAI Research Papers, 2019, No. 13.
4. Borgogno, O.; Colangelo, G., *Data Sharing and Interoperability Through APIs: Insights from European Regulatory Strategy*, in *Computer Law & Security Review*, 2019, vol. 35, issue 5.
5. Borgogno, O.; Colangelo, G., *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, in *European Business Law Review*, 2020, 31, no. 4, pp. 573-610.
6. Crisanto, J.C.; Ehrentraud, J.; Fabian, M., *Big techs in finance: regulatory approaches and policy options*, FSI Briefs, 2021, No. 12.
7. De la Mano M.; Padilla, J. *Big Tech Banking*, in *Journal of Competition Law and Economics*, 2018, 14(4), pp. 494-526.
8. Di Porto, F.; Ghidini, G.*, "I Access Your Data, You Access Mine": Requiring Data Reciprocity in Payment Services*, in *International Review of Intellectual Property and Competition Law - IIC*, 2020, 51, pp. 307-329.
9. Franck, J-U.; Peitz, M., *Market Definition in the Platform Economy*, CRC TR 224 Discussion Paper Series, 2021.

---

enforcement to challenge potential anti-competitive practices carried out by incumbent as well as new entrants".

71 On this issue, see Pardolesi, R., *Tutto (o quasi) quel che avreste voluto sapere sul principio del consumer welfare in diritto antitrust* (Mar. 5, 2021), [http://www.law-economics.net/workingpapers/L&E-LAB-COM-59-2021.pdf], Accessed 18 June 2021.

10. Gozman, D.; Hedman, J.; Olsen, K.S., *Open Banking: Emergent Roles, Risks & Opportunities*, in AISel Research Papers, 2018, No. 183.
11. Graef, I.; Husovec, M.; van den Boom, J., *Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, in *Journal of European Consumer and Market Law*, 2020, 9(1), pp. 3-16.
12. Gupta, P; Tham, T.M., *Fintech. The New DNA of Financial Services,* de Gruyter, Boston-Berlin, 2019.
13. Hermes, S.; Pfab, S.; Hein, A.; Weking, J.; Böhm, M.; Krcmar, H., *Digital Platforms and Market Dominance: Insights from a Systematic Literature Review and Avenues for Future Research*, PACIS 2020 Proceedings, 42.
14. Hovenkamp, H.J., *Antitrust and Platform Monopoly*, U of Penn, Inst for Law & Econ, Research Paper No. 20-43.
15. Kaufman Winn, J.; Wright, B., *The Law of Electronic Commerce*, 4th ed., Wolters Kluwer, New York, NY, 2021, § 7.09[B].
16. Liu, H.-W., *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and its Open Banking Watershed Moment*, 30 Wash. Int'l L.J. 28, 31 (2020).
17. Paal, B.P., *Market Power in Data (Protection) Law*, in *Global Privacy Law Review*, 2021, vol. 2, issue 1, p. 15.
18. Padilla, J., *BigTech "banks", financial stability and regulation*, in *Estabilidad financiera*, 2020, issue 38, pp. 11-26.
19. Sarmas, I., *Market Definition for Two-Sided Platforms: Why Ohio v. American Express Co. Matters for the Big Tech*, 19 Fla. St. U. Bus. Rev. 199 (2020).
20. Santesteban, C.; Longpre, S., *How Big Data Confers Market Power to Big Tech: Leveraging the Perspective of Data Science*, in *The Antitrust Bulletin*, 2020, vol. 65, issue 3, pp. 459-485.
21. Sitaraman, G., *Too Big to Prevail: The National Security Case for Breaking up Big Tech*, 99 Foreign Aff. 116 (2020).
22. Stiefmueller, C.M., *Open Banking and PSD 2: The Promise of Transforming Banking by 'Empowering Customers'*, in Spohrer, J.; Leitner C. (eds.), *Advances in the Human Side of Service Engineering. AHFE 2020. Advances in Intelligent Systems and Computing*, vol. 1208, Springer, Cham, 2020, pp. 299-305.
23. Vandenborre, I.; Levi, S.D.; Janssens C., *Fintech and access to data*, in *Concurrences*, 2019, N° 4, p. 3.
24. Vezzoso, S., *Fintech, access to data, and the role of competition policy*, in Bagnoli, V. (ed.), *Competition and Innovation*, Scortecci, São Paulo, 2018, p. 32.
25. Zunzunegui, F., *Digitalisation of Payment Services*, Ibero-American Institute for Law and Finance, Working Paper Series, No. 5/2018, p. 26.

WEBSITE REFERENCES

1. Borgogno, O.; Colangelo, G., *The data sharing paradox: BigTechs in finance*, [https://ssrn.com/abstract=3591205], Accessed 18 June 2021.

2. Borgogno, O.; Colangelo, G., *Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking*, [https://ssrn.com/abstract=3513514], Accessed 18 June 2021.
3. Mersch, Y., Lending and payment systems in upheaval - the fintech challenge, speech given at the 3rd annual Conference on Fintech and Digital Innovation, Brussels, 26 February 2019 [https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190226~d98d307ad4.en.html], Accessed 18 June 2021.
4. Pandy, S., *Modernizing U.S. Financial Services with Open Banking and APIs* (Feb. 8, 2021) [https://www.bostonfed.org/publications/payment-strategies/modernizing-us-financial-services-with-open-banking-and-apis.aspx], Accessed 18 June 2021.
5. Pardolesi, R. *Tutto (o quasi) quel che avreste voluto sapere sul principio del consumer welfare in diritto antitrust* (Mar. 5, 2021), [http://www.law-economics.net/workingpapers/L&E-LAB-COM-59-2021.pdf], Accessed 18 June 2021.
6. Vallabhaneni, P., *CFPB Seeks Comments on Highly Anticipated Consumer Access to Financial Information Rulemaking* (Nov. 3, 2020), [https://www.whitecase.com/publications/alert/cfpb-seeks-comments-highly-anticipated-consumer-access-financial-information], Accessed 18 June 2021.