Open Finance and Consumer Protection: uneasy bedfellows[1]

Federico Ferretti[2] and Peter Petkoff[3]

Abstract

Summary

1. Introduction. – 2. Information to financial markets, data and innovation. – 2.1. Traditional information to markets. 2.2. – Technology, open innovation and new market structures. – 3. Regulation as enabler for innovation: Open Banking. – 4. From Open Banking to Open Finance. – 4.1. – The cohabitation between the PSD2 model and the GDPR. – 4.2. – The proposal for a Data Act. – 4.3. – The approach in the United Kingdom. – 5. Open Risks. – 5.1. Legal uncertainty and the lack of effective control. – 5.2. Black boxes and dark patterns. – 6. Conclusions

1. Introduction

This paper investigates the challenges posed by Open Finance in its quest to place consumers at its centre by empowering and protecting them. It questions the extent to which the envisaged legal framework is capable of offering the tools to achieve such goals.

Information to financial service markets has been crucial for long time. However, its function is undergoing a deep transformation. As the financial services industry embraces digitalisation, financial service providers use increasing data analysis and profiling to target customers, offer them

[1] This research has been carried out within the Jean Monnet Chair in Digital Market Law (E-DSM) E-DSM - 101047038 - GAP-101047038. The European Commission's support for the research does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. Sections 1, 2, 3, 4.1, 4.2, 5, and 6 are attributed to Federico Ferretti and Section 4.3 to Peter Petkoff.

[2] Jean Monnet Professor in Digital Market Law at *Alma Mater Studiorum* University of Bologna (IT).

[3] Research Fellow at the University of Oxford and Senior Lecturer in Law at Brunel University London (UK).

customised products with personalised pricing, and create new products or services. Technological innovation has become the key aspect for new models in the provision of finance.[4]

Open Finance is the late frontier of the financial services' industry. Upon enabling legislation, it will refer to the obligation for traditional financial service providers to open access to their customers' financial data to third-party providers ('TPP') and share the data with them for the provision of a wider range of the same financial products or services, or the creation of new ones. It aims to expand TPP access to, and sharing of, the whole spectrum of financial data sources taken from a variety of financial providers and product lines such as savings, mortgages, consumer credits, investments, pensions, insurance, advice, etc. So devised, Open Finance advances significantly the transition to data-driven finance and may reshape the EU financial services industry.

So far, digital innovation and competition have been the thrust for the enactment of the late rich body of EU law which is currently being developed in response to the digital age.[5] At the same time, under EU policy, for Open Finance to exist customers need to factually control their data and be protected from abuses or misuses.[6]

However, data control, consumer empowerment and protection, and the processing of large amounts of diverse data in finance raise policy and legal issues. Regulation plays a pivotal role in the shaping of a EU single market fit for a sustainable digital economy, ensuring an optimal economic and social balance. The aim of this work is to analyse the extent to which the intersection of current and envisaged legal instruments may offer suitable solutions to achieve the envisaged policy goals and tackle the risks likely to be opened by Open Finance.

To reach its goal, this work is construed as follows.

---

[4] CAPRIGLIONE F, "The financial system towards a sustainable transition", 10(1) *Law and Economics Yearly Review* (2021), 1.

[5] E.g. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35–127; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56–83; Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

[6] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, COM(2020) 591 final; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU, COM/2020/592 final; European Commission, Targeted consultation on open finance framework and data sharing in the financial sector, available at https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-open-finance_en.

Section 2 sets the theoretical foundations of data sharing in the financial services domain to show the transformative type and use of data to the changing economic cycle. It provides the necessary context of the new market structures in the transition towards open innovation and data-driven finance. Section 3 explores the role of regulation as enabler of innovation. It shows how the provisions of the Payment Services Directive 2 have instituted the new market model of Open Banking, presenting to the reader the mingling between banking and the data business as the forerunner of Open Finance, where the whole financial service sector becomes involved. Like Open Banking, Open Finance is a concept enabled by legislation. Thus, drawing from the experience of Open Banking, Section 4 examines the difficult intersection between the legislative model of the PSD2 and data protection law. Equally, it studies the proposal for a Data Act as a regulatory initiative on fair access and use of data of general application with whom Open Finance specific regulation will need to coexist. The approach taken in the neighbouring jurisdiction of the United Kingdom ('UK') is also presented to show the feasibility of a functional alternative policy debate. Section 5 sets forth the risks identified from the legal analysis, advancing that the resulting legal uncertainty, coupled with weak legal instruments may pose great risks for consumers, especially in a complex environment susceptible to opacity and dark patterns, where vulnerabilities thrive. Section 6 concludes.

2. Information to financial markets, data and innovation

2.1.Traditional information to markets

Finance has long been an information industry. It is a common feature that financial institutions process and exchange a growing amount of personal financial data about their customers as part of their business models. For example, lenders and insurers access databases managed by sectoral associations or third-party providers (e.g. Credit Bureaus) in order to evaluate a consumer's application, the risks involved in a transaction and their management, or the prospective customer's creditworthiness or trustworthiness.[7]

Traditionally, the type of data exchanged are those of the concerned product line for the benefit of the concerned market players. For example, in credit relationships, traditional data are personal data relating to debt payments and financial accounts with lenders. But the level of product coverage in the databases differs from country to country.[8]

[7] SCIARRONE ALIBRANDI A and MATTASSOGLIO, F, "Le centrali dei rischi: problemi e prospettive", 4 Diritto della Banca e del Mercato Finanziario (2017), 764; FERRETTI F, *The law and consumer credit information in the European community: the regulation of credit information systems* (Routledge, 2008).

[8] ACCIS, *ACCIS 2020 Survey of Members – An Analysis of Credit Reporting in Europe* (2015).

Likewise, in the insurance sector traditional data are those relating to the insured risk, e.g. the behaviuor of a customer that is likely to cause the event.

In financial circles, the virtues of data sharing are usually portrayed in terms of more efficient processes and decision-making, or for a better management of financial risks or fraud situations. Most of the times, the benefits for consumers have been highlighted in terms of products/services better tailored to their needs, better quality, or cost-efficiency.[9] Moreover, the extensive use of financial data has been promoted to achieve a number of policy objectives. These include the facilitation of the access to more affordable and better-quality financial services for consumers,[10] the prevention of consumer over-indebtedness by limiting irresponsible/predatory lending,[11] and the contribution to financial stability by limiting financial institutions' loss risks.[12]

Under certain national systems, financial data can even be part of a broader information centralisation system managed by national central banks for the purpose of oversight of the financial system as a whole, i.e. they are an instrument for the prudential supervision of the financial system.[13]

Supported by classical economic and financial literature, dominant justifications for data sharing have started with the reduction of the information asymmetry between financial providers and borrowers for a better risk analysis, including problems of bad selection of customers, and the risk which arises from the characteristics of prospective customers that may increases the possibility of an economic loss.[14]

It is from this classic economic theory that the first correlations or associations have started to emerge, in particular the one that past behaviour is predictive of future behaviours.[15] Contrary to causation,

---

[9] E.g. Bank of England, "Should the availability of UK credit data be improved?", *Discussion Paper* (May 2014); HM Treasury, *Improving access to SME credit data: summary of responses* (June 2014), at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/323318/PU1681_final.pdf; TURNER M and VARGHESE R, *The Economic Consequences of Consumer Credit Information Sharing: Efficiency, Inclusion, and Privacy* (OECD, 2010); . JENTZSCH N, *Financial Privacy - An International Comparison of Credit Reporting Systems* (Springer, 2007).

[10] OECD, *Facilitating access to finance - Discussion Paper on Credit Information Sharing*, at https://www1.oecd.org/globalrelations/45370071.pdf

[11] ACCIS, *ACCIS Response to Financial Services User Group (FSUG) Position Paper on the London Economics Study on Means to Protect Consumers in Financial Difficulty* (October 2013), at http://www.accis.eu/uploads/media/ACCIS_Response_to_FSUG_Position_Paper_October_2013.pdf.

[12]World Bank, *General principles for credit reporting* (Washington DC, 2011) http://documents.worldbank.org/curated/en/662161468147557554/General-principles-for-credit-reporting.

[13] JAPPELLI T and PAGANO M, "Public Credit Information: A European Perspective", in Miller MJ (ed.), *Reporting systems and the international economy*. (MIT Press, 2003), 81-114.

[14] STIGLITZ JE and WEISS A, "Credit Rationing in Markets with Imperfect Information", 71(3) *American Economic Review* (1981), 393-410; BERGER AN and UDELL GF, "Relationship Lending and Lines of Credit in Small Firm Finance", 68 *Journal of Business* (1995), 351-381; AKELOF G, "The market for 'Lemons': Quality uncertainty and the market mechanism", 28(3) *Quarterly Journal of Economics*, (1970), 523–547; DIAMOND DW, "Monitoring and Reputation: The Choice between Bank Loans and Directly Placed Debt", 99(4) *Journal of Political Economy* (1991), 689-721; ADMATI AA and PFLEIDERER PC, "Forcing Firms to Talk: Financial Disclosure Regulation and Externalities", 13 *Review of Financial Studies* (2000), 479-519.

[15] MILLER MJ, "Introduction", in Miller MJ (ed.), *Reporting Systems and the International Economy* (MIT Press 2003), 1-23.

under these assumptions the observation of human past through the data has been deemed to statically or repeatedly predict the likelihood of the future.

Such correlations also explain how economic theory has then moved to advance the proposition that data exchanges among financial service providers could play a major role as a customer's discipline device. Customers would know that the causation of an event, change in circumstances, or a delay or a default in re-payment compromise their reputation with all the other providers on the market, resulting in credit or insurance with more costly terms or by cutting them off from the market entirely.[16] Therefore, data sharing has been seen as reducing moral hazard. A customer's 'good name', i.e. their reputation collateral, contributes to provide an incentive to maintain certain behaviours or meet commitments much the same way as does a physical collateral.[17]

From another angle, the sharing of data on customer relationships has been also promoted to reduce the information monopoly of individual providers and the competitive advantage of large financial institutions, thus promoting market competition.[18] The problem of asymmetric information and adverse selection becomes greater for new market entrants, particularly providers from other Member States. This is particularly the case in the context of the EU single market and cross-border entry or cross-border provision of financial services. In addition to competitive disadvantages in relation to incurring greater risks of incorrectly estimating a customer's risk, without relevant information on customers new market entrants would be likely to attract precisely those who were rejected or overpriced by existing providers in the market.[19] This circumstance has induced recent literature to conclude that personal data exchanges, market structure, and competitive conduct are intrinsically intertwined in the financial services market. From the standpoint of industrial organisation, the availability of data shared by the sector can affect firms' choice not only of whether to entry another jurisdiction but also the mode of doing it, i.e. whether through the cross-border provision of services, the setting-up of branches or subsidiaries, or through mergers and acquisitions.[20]

One of the most apparent limitations of the above theoretical foundations lies in the neo-classical understanding or bias of the consumer as purely a *homo economicus* where they are seen as rational, informed, narrowly self-interested, vigilant and alert economic agents. In short, consumers who have the ability to make judgments towards their subjectively defined ends and who maximise their own utility and make intelligent and conscious choices, free of external events biasing or forcing their

[16] JAPPELLI T and PAGANO M, "Information Sharing, Lending and Defaults: Cross-Country Evidence", 26(10) *Journal of Banking and Finance* (2002), 2017-2045.
[17] MILLER, *supra* note 15.
[18] European Commission, *Report of the Expert Group on Credit Histories* (Brussels, May 2009).
[19] GIANNETTI C, JENTZSCH N, SPAGNOLO G, "Information-Sharing and Cross-Border Entry in European Banking", *ECRI Research Report N. 11* (Brussels, February 2010).
[20] *Ibid.*

behaviour.[21] Such an economic interpretation appears inconsistent with the findings and increasing acceptance of the behavioural literature which attempts to explain relevant features of human behaviour and the consumers' cognitive limitations that cannot be explained under standard economic assumptions. It challenges economic assumptions by using a number of alternative social sciences or disciplines such as psychology, sociology, neurosciences to explore the real behaviour of human beings and how economic decisions are taken or dictated in the economic, cultural, and social context where they live.[22] Under this perspective, traditional financial data may only give a partial or fragmented picture of a customer's story or situation. They may present a distorted impression of individuals, not because the data are incorrect but for presenting a piecemeal picture making it seem incomplete and incorrect. In simple language, it is like taking a few silvers of a person and presenting that as the whole her/him.

Many other questions arise on the viability and assessment of those who are not in the databases. Arguably, those who are not in the databases or lack information for not having incurred into any financing operation are not negligible in numbers. Such a data sharing seems to penalise those segments of the population with a weaker financial history notwithstanding their personal circumstances, or ignoring behavioural biases or unstandardised conducts. From this point of view, the resulting theories appear to some extent artificial. The inability of these systems to detect atypical behaviours raises questions and problems because they also make assumptions about what 'normal' behaviour is, where deviation from the established pattern is seen as undesirable or questionable, with all the following implications.

The use of personal data in the same financial product line - combined with the limitations or errors in the data and in the analytic tools – could also raise questions around the relationship between the data and pricing practices, for example making use of analytical data showing a consumer's degree of willingness to pay more, liaising higher prices to higher perceived risks of a consumer, or

[21] STATEN ME and CATE FH, "Does the Fair Credit Reporting Act Promote Accurate Credit Reporting?", *Working Paper Series BABC 04-14*, *Joint Center for Housing Studies* (Harvard University, February 2004); BECKER GS, *The economic approach to human behavior* (University of Chicago Press, 1976); OSOVSKY A, "The misconception of the consumer as a homo economicus: a behavioral-economic approach to consumer protection in the credit-reporting system", 46(3) *Suffolk University Law Review* (2013), 881–933.

[22] The literature on behavioural economics is copious. Examples are JOLLS C, SUSTAIN CR, THALER R, "A behavioral approach to law and economics", 50 *Stanford Law Review* (1998), 1471–1550; DIAMOND P, and VARTIAINEN H (eds.), *Introduction to behavioural economics and its applications* (Princeton University Press, 2007); CAMERER C, ISSACHAROFF S, LOEWENSTEIN G, O'DONOGHUE T, RABIN M, "Regulation for conservatives: behavioral economics and the case for asymmetric paternalism", 151 *University of Pennsylvania Law Review* (2003), 1211–1254; HANSEN J and KYSAR D, "Taking behaviouralism seriously: the problem of market manipulation", 74 *New York University Law Review* (1999), 630–749. For literature specifically addressing borrowers' behavior see AGARWAL S and ZHANG J, A review of credit card literature: perspectives from consumers (19 October 2015), at https://www.fca.org.uk/publication/market-studies/review-credit-card-literature.pdf; LEA S, *Behaviour Change: Personal Debt* (The British Psychological Society, no date), at www.bps.org.uk/behaviourchange; XIAO J, *Consumer Economic Wellbeing* (Springer, 2015); WRIGHT J, "Behavioral law and economics, paternalism, and consumer contracts: an empirical perspective", 2 *NYU Journal of Law and Liberty* (2007), 470-511.

demonstrating their inertia to switch products or services. In this respect, the biases behind the classic economic theories go against the foundations of human behaviours as heterogeneous and unpredictable.

2.2. Technology, open innovation and new market structures

As the underwriting of financial services and technologies evolve, and finance adapts to changing economic cycles and demographics, new business models recognise the limits of traditional data.

A limit of traditional data is that they are largely of historical nature. As they make use of a limited number of categories of data, they do not provide a reliable picture.

Technological innovation thus becomes the key to develop new models in the provision of personal finance.[23]

Technologically enabled financial innovation in consumer financial services ('fintech') capable of making use of large datasets from various unrelated sources ('big data') are one important facet of late innovations that is generating significant interest in financial markets for its possible disruptive effects in the sector.[24] Many Fintech developments are based on proprietary artificial intelligence systems (AI) and associated innovative uses of data. AI embraces different forms of computer systems that are able to learn from the data and their own experiences to solve complex problems or uncover patterns to predict future data or perform decision-making tasks (also known as machine-learning powered by mathematical algorithms able to create further algorithms based on accumulated data).[25]

As technologies evolve, and standards and appetite for financial services adapt to changing economic cycles and shifting demographics, a wider array of new data become available for analysis. These other data are those data gathered from diverse sources outside the standard product lines that financial institutions used to evaluate their clients. Their volume is greater than that of the traditional sources as they are usually taken from several data points mined from consumers' digital or offline activities. Even if such big data are not intuitively related to the product line and specific transactional risk, all data become financially relevant data with an open nature as to their sources. This also enables the leverage of a large volume of data from diverse sources and generated from various transactions to create new products or business models. The analysis of big data, increasingly in real time, drives

[23] BASKERVILLE R, CAPRIGLIONE F and CASALINO N, "Impacts, challenges and trends of digital transformation in the banking sector" 9(2) *Law and Economics Yearly Review* (2020), 341.

[24] European Banking Authority, *Discussion Paper on innovative uses of consumer data by financial institutions* (London, 4 May 2016); European Banking Authority, *EBA Guidelines on creditworthiness assessment", Final Report on Guidelines on Creditworthiness Assessment* (London, 19 August 2015); The Financial Inclusion Centre, FinTech – Beware of the "Geeks' Bearing Gifts?", *A Financial Inclusion Centre Discussion Paper* (January 2018).

[25] CAPRIGLIONE F, "Law and economics. The challenge of artificial intelligence", 10(2) *Law and Economics Yearly Review* (2021), 189. See also MURPHY KP, *Machine Learning: A Probabilistic Perspective* (MIT Press, 2012); LANDAU M, "Artificial Intelligence and Machine Learning: How Computers Learn", *Tech Innovation* (17 August 2016), available at https://iq.intel.com/artificial-intelligence-and-machine-learning/

knowledge and value creation across society in the fashion of a so-called 'open innovation', that is an innovation ecosystem where ideas and knowledge flow across firm boundaries sourced from both internal and external sources by means of sharing knowledge and information.[26]

These innovative techniques are capable of reshaping business models, underwriting criteria, and customer experiences. Their innovations associate the commoditization of big data analytics with an understanding of demographic changes, borrower needs, and how to connect to customers through new technological channels.[27] Reportedly, the 2008 financial crisis first, and the COVID-19 pandemic next, also have played an accelerating role marking the impetus and arrival of new market players pushing for competition over innovation to lower costs and gain market share.[28]

The fundamental drawback of the resulting market physiognomy is that data holders could legitimately refuse access to their data infrastructures on grounds of intellectual property protection, data protection concerns, security risks, or the permanence of unclear rules over liabilities towards the customers.[29]

The fintech ecosystem thus risks displaying low competition characterised by low elasticity of demand, lock-in problems, and exclusivity of services of mainstream providers,[30] as well as a legal vacuum of an alternative market operating outside the relationship between the traditional incumbents and their customers.[31]

3. Regulation as enabler for innovation: Open Banking

[26] CHESBROUGH HW, *Open Innovation: The new imperative for creating and profiting from technology* (Harvard Business School Press 2003).

[27] PricewaterhouseCoopers, *Is it time for consumer lending to go social?* (February 2015), at https://www.pwc.lu/en/fintech/docs/pwc-fintech-time-for-consumer-lending-to-go-social.pdf

[28] ZETZSCHE DA, BUCKLEY RP, ARNER DW and BARBERIS JN, "From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance", *EBI Working Paper Series n. 6* (2017); MALVAGNA U and SCIARRONE ALIBRANDI A (eds), *Sistema Produttivo e Finanziario Post COVID-19: dall'Efficienza alla Sostenibilità* (Pacini Giuridica, 2021).

[29] European Commission, *Towards an integrated European market for card, Internet and mobile payments*, COM (2011) 941 final. See also COLANGELO G and BORGOGNO O, 'Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule', 31 *European Business Law Review* 2020, p (573).

[30] European Commission, 'Commission staff working document Impact Assessment accompanying the Proposal for a directive on payment service in the internal market', SWD (2013) 288 final; European Central Bank, 'Financial Stability Review November 2016 – Special Feature' (2016), at https://www.ecb.europa.eu/pub/pdf/fsr/financialstabilityreview201611.en.pdf; UK Competition and Market Authority, 'The Retail Banking Market Investigation Order 2017' (2017), at https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017; The Netherlands Authority for Consumers and Markets, 'Barriers to entry into the Dutch retail banking sector' (2014), at https://www.acm.nl/sites/default/files/old_publication/publicaties/13257_barriers-to-entry-into-the-dutch-retail-banking-sector.pdf.

[31] European Banking Authority, 'Discussion Paper on the EBA's approach to financial technology (FinTech)', *EBA/DP/2017/02* (4 August 2017).

Regulation can take a key role in enabling innovation in financial services and opening financial markets.

So far, in the EU this targeted regulation has been limited to the banking payments sector.

As the data business permeates the global economy, banking and electronic payment services represent a frontier very exposed to competitive pressures from the infant fintech industry. For some time, payments have been characterised by electronic fund transfer systems having gone through the transition from paper payment services (e.g. cash, bank cheques, traveller's cheques, etc.) to electronic means. In the digital economy, payment accounts and data have become an essential source from which services can be provided, not only by banks but also by new market players capable of extracting value from them competitively.[32]

The thrust towards innovation and competition in a market traditionally dominated by the banking sector has motivated the substantial revision and reordering of the regime formerly established by the foregoing Payment Services Directive ('PSD1').[33] The late legislative intervention of the Payment Services Directive 2 ('PSD2')[34] has modernised the regulation of payment transactions and consumer protection to the changing needs brought by digitalisation.[35] It intervenes in the single payments market enabling a new banking model called 'Open Banking'.

Open Banking is not a technology-based concept but one of legal derivation. This model refers to the obligation under the PSD2 for banks to open access to their customers' payment accounts, banking transactions, and other financial data using interoperable interfaces ('Application Programming Interfaces') to third-party service providers ('TPP'). The PSD2 lays down the normative terms for the achievement of integrated retail payments in the EU that are inclusive of existing and new payment services delivered by new market players. Its ambitious goal is to take advantage of innovative technology-enabled solutions (fintech) to generate efficiencies and reach a broader market

[32] MAVROMATI D, *The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market* (Alphen aan den Rijn: Kluwer Law International 2008); JANCZUK-GORYWODA A, 'Evolution of EU Retail Payments Law', 40 *European Law Review* 2015, 858; GRIMIGLIANO G, 'The Lights and Shadows of the EU law on Payment Transactions', in G Grimigliano (ed.), *Money, Payment Systems and the European Union* (Cambridge: Cambridge Scholars Publishing 2016), p 25; VARDI N, 'Regulation of Payments after the PSD: Is there still a Role for Domestic Law', in G Grimigliano (ed.) *Money, Payment Systems and the European Union* (Cambridge: Cambridge Scholars Publishing 2016), 39.

[33] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, 1–36.

[34] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, 35–127.

[35] See, in particular, Recital 95 PSD2.

with more choice and integrated services. At the same time, it aims to pursue transparency and consumer protection.[36]

Thus, regulation has not just allowed, but it has mandated data access and sharing to develop a novel market model in the area of payments, in which traditional banking meets and is transformed by the data economy and the competition of innovative fintech firms. Mandating data access and sharing through regulation, the EU shifts the single market approach towards digitalisation and competition. Customers are required to grant consent to let the bank allow such access. Third-party providers can then use the customer's shared data. So doing, this model breaks the concentration of information in traditional banks, and allows the networking of accounts and data across a novel sector made of traditional and new service providers. Fresh competition is created for a more efficient provision of existing services, as well as the development of new ones.[37]

Examples are new methods of mobile payments or the delivery of complimentary personalised financial services such as financial advice, loans, insurance products. New uses may include comparing the customer's accounts and transaction history to a range of financial service options, aggregating data to create marketing profiles, or making new transactions and account changes on the customer's behalf. Shared data can facilitate the process of switching from using one bank's account to another bank's account. Financial service providers can look at consumers' transaction data to identify the best financial products and services for them, such as new accounts that would earn a higher interest rate than the current account or different credit cards with a lower interest rate. Providers may get a more accurate picture of a consumer's financial situation and risk level to offer more profitable financial terms. New services may help consumers get a more accurate picture of their own finances before taking on debt or other financial services.

Broadly, the PSD2 operates on two interrelated levels.

At first, it intervenes in the establishment, authorisation, and supervision of payment firms and the regulation of payment transactions. Adjusting to the digital market, it enlarges the scope of coverage of the law, it clarifies the extent of consumer rights and service provider obligations, and it reinforces security and authentication requirements.[38]

---

[36] Recital 6, PSD2.

[37] On Open Banking see e.g. COLANGELO G and BORGOGNO O, 'Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule', 31 *European Business Law Review* 2020, p (573); European Banking Authority, 'Discussion Paper on innovative uses of consumer data by financial institutions', *EBA/DP/2016/01* (4 May 2016); RABITTI M and SCIARRONE ALIBRANDI A, "I servizi di pagamento tra PSD2 e GDPR: Open Banking e conseguenze per la clientela", in F Capriglione (a cura di), *Liber Amicorum Guido Alpa* (CEDAM, 2019), 711-735; CIRAOLO F, *Open Banking, Open Problems.* Aspetti controversi del nuovo modello dei "sistemi bancari aperti", IV Rivista di Diritto Bancario (2020), 611.

[38] See the various provisions of Titles II, III and IV of the PSD2.

Next, it recognises and regulates those TPP emerging from new fintech realties in payment services, bringing them under the same harmonised standards, requirements, and obligations on an equal footing with the traditional payment providers regardless of the business model they apply.[39] Introducing the so-called 'access to account rule', it opens the market to new services by granting TPP access to the customers' payment accounts held in the banks. The latter must allow TPP authorised by the competent authority in their home Member State[40] access to the data contained in payment accounts in real time on a non-discriminatory basis.[41] By accessing and exploiting the large quantity of real-time data of the banking realm, technology firms have started disrupting retail financial markets.[42]

The 'access to account rule' has therefore become the tool to unlock the data power of banks over innovative fintech firms. Access by TPP is to 'payment accounts' only, defined as accounts "held in the name of one or more payment service users *(…)* used for the execution of payment transactions".[43] Savings accounts and other non-payment accounts seem therefore excluded from the application of the PSD2.[44]. Access to payment accounts shall take place in a secure way under the guidelines laid down by the European Banking Authority.[45] Any access may occur only upon conclusion of a contractual relationship between the account holder and a TPP, unusually framed as 'explicit consent' by the PSD2, precisely for the purpose of providing those kinds of services that need the data contained in the account.[46] Under the PSD2, TPP are subject to conduct of business restrictions and requirements that do not allow them to hold the payer's funds in connection with the service, store

[39] Recitals 27-33 PSD2.
[40] Art. 36 PSD2.
[41] Art. 64 to 68 PSD2.
[42] BORGOGNO O and COLANGELO G, 'The data sharing paradox: BigTechs in Finance', (2020) 16 *European Competition Journal* 492; BORGOGNO and COLANGELO G, 'Consumer Inertia and Competition-sensitive Data Governance: The Case of Open Banking' (2020) 4 *Journal of European Consumer and Market Law* 143; DI PORTO F and GHIDINI G, 'I access your data, you access mine. Requiring data reciprocity in payment services' (2020) 51 *IIC - International Review of Intellectual Property and Competition Law* 307.
[43] Art. 4(12) PSD2.
[44] This circumstance also finds support in Case C-191/17, *Bundeskammer für Arbeiter und Angestellte v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG* [2018] EU:C:2018:809 where the Court confirmed that accounts which allow for sums deposited without notice and from which payment and withdrawal transactions may be made solely by means of a current account do not come within the concept of payment account.
[45] Art.95 PSD2, followed by European Banking Authority, *Final draft RTS on SCA and CSC under PSD2 (EBA-RTS-2017-02)* (23 February 2017); Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication C/2017/7782, OJ L 69, 13.3.2018, p. 23–43; European Banking Authority, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04)* (13 June 2018).
[46] For Payment Initiation Services, see Art. 66 PSD2, stating that "when the payer gives its explicit consent for a payment to be executed and (*omissis*)"; for Account Information Services, see Art. 67 PSD2 providing that "the account information service provider shall: (a) provide services only where based on the payment service user's explicit consent; (*omissis*)".

sensitive payment data of the service user, or process data beyond that necessary to provide the service.[47]

These provisions have given rise to a market model that shifts from the money business to the data business and vice versa, where account data are shared with new market players of the fintech industry capable of capturing or creating value around existing un- or under-exploited assets.[48]

In the Open Banking model, therefore, the new paradigm reflects the unbundling of the provision of financial services in more market segments, and the disintermediation of the banking industry. The latter, however, becomes key in the Open Banking ecosystem, assuming a new form of forced intermediation between the service user (the account holder) and the fintech TPP. The services can only exist via the traditional providers, creating a new market structure where the latter become digital platforms for the distribution of financial services. They facilitate and create a dependency for the contractual interactions of two or more market agents, but without having any contractual relationship with one of them (the TPP), at the same time allowing the other one (the customers) to continue the fruition of their own services.

The Open Banking environment thus generates indirect network effects, making possible bilateral ventures otherwise not attainable with other means,[49] at the same time producing new dependencies. In this way, the Open Banking market structure moves towards a confluence between traditional financial service providers becoming technological firms (but still on the money business) and technological firms entering the financial services market, where the latter may be infant fintech businesses or established technological giants already dominating the data service market (the so-called 'Tech-Fin' or 'Big-Tech').[50]

From this angle, the PSD2 is the law that encourages an expanding use of personal data and enables a vast array of newcomers to access increasingly more data sources for novel purposes.

---

[47] Art. 66(3) PSD2.

[48] CHESBROUGH H, 'Business Model Innovation: Opportunities and Barriers', 43 *Long Range Planning* 2010, 354.

[49] ZACHARIADIS M and OZCAN P, 'The API economy and digital transformation in financial services: the case of Open Banking', *SWIFT Institute Working Paper No. 2016-001*, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199; D MILANESI, 'A new banking paradigm: the state of Open Banking in Europe, the United Kingdom and the United States', *TTLF Working Papers No. 29, Stanford-Vienna Transatlantic Technology Law Forum* (2017), from https://law.stanford.edu/publications/a-new-banking-paradigm-the-state-of-open-banking-in-europe-the-united-kingdom-and-the-united-states/

[50] ZETZSCHE D ET AL, *EBI Working Paper Series n. 6*, 2017; DI PORTO and GHIDINI, *supra* note 42; STULZ RM, 'FinTech, BigTech, and the future of banks', *NBER Working Paper No. 26312* (2019), at https://www.nber.org/papers/w26312. For example, note that Google has secured an e-money license after Lithuania granted authorisation. The license enables the company to process payments, issue e-money, and handle electronic money wallets. It gives permission to operate across the EU via the passporting rights system. Likewise, Facebook and Amazon obtained licenses in Ireland and Luxembourg. See SEPUTYTE M and KAHN J, "Google Payment Expands With E-Money License From Lithuania", *Bloomberg* (21 December 2018), at https://www.bloomberg.com/news/articles/2018-12-21/google-payment-expands-with-e-money-license-from-lithuania.

True, payment accounts contain a vast amount of data for analysis, from financial data relating to incoming and outgoing transactions, balances, preferences, patterns, dependencies, behaviours, aspects of the social life, etc. They can be an exceptional tool for consumer profiling and predictive purposes. At the same time, however, they can also reveal behavioural biases and vulnerabilities in all aspects of consumers' life, especially if integrated with data from other unrelated sources and processed by algorithms powered by artificial intelligence technologies.

4. From Open Banking to Open Finance

Following the opportunity provided by the PSD2 of opening-up bank account data for TPP access, the EU legislator plans to extend the Open Banking model gradually in a transition to data-driven finance to a broader range of financial services. As part of the priorities of the Digital Finance Strategy to promote data-driven innovation in finance, the EU aims to establish a common financial data space through a number of more specific measures.[51] Of relevance here is the priority to create enhanced data sharing and access to, and reuse of, data in the financial sector paving the way to 'Open Finance'. Upon enabling legislation, Open Finance will be the next step in the evolution of Open Banking, whose reach becomes expanded by empowering consumers with further control over their data and granting TPP access to more data sources for a wider range of financial services such as savings, mortgages, consumer credit, investments, pensions, insurance, financial advice, etc. It extends the delivery of digital financial services via interoperable interfaces, creating new fintech industries, and developing further service disintermediation and new forms of data intermediation. With Open Finance it is created a networked system that is no longer limited to payment services but that relies on the ability to leverage a broad range of financial institutions' infrastructures to provide a financial service that the provider does not offer to consumers outside of its existing footprint.
As for Open Banking, the key element to enable Open Finance is the regulation to be implemented.

4.1.The cohabitation between the PSD2 model and the GDPR

The starting point about the nature of a legislative framework for Open Finance is rooted in the consolidation and extension of Open Banking-like legislation, as well as overlapping legislation relating to data.

[51] Digital Finance Strategy, *supra* note 6.

As a consumer-centric business model, from the angle of consumer protection the most important building block of Open Finance is that of consumers' control of the data pertaining to them.

Consumer financial data processing triggers the application of the GDPR, thus overlapping with a PSD2-like and creating a legal environment where financial regulation and data regulation blend. Therefore, the question of whether this blended regulation is robust enough to foster a transition to Open Finance becomes essential.

As a EU Regulation, the GDPR has direct effect designed to eliminate risks of national particularities and diversity of practices, which would frustrate the goal of achieving uniformity.

Prima facie the principal purposes of the PSD2 model and the GDPR are in contrast one another, with the former endorsing the stimulus for expansive data sharing, whilst the latter protecting and restricting the freedom to share them.

In the absence of derogations, it is in light of the significance of data protection legislation that one should read the processing of big data in financial services, including data in Open Finance.[52]

The GDPR formulates the conditions under which information processing is legitimate.

Among the many aspects regulated by the GDPR, some require attention for their overlap with the PSD2 model.

Within the respect of the key principles of purpose limitation and data minimisation,[53] the GDPR sets the legal requirements for a valid basis for legitimate data processing. A data controller must be able to provide a base for the processing activity only if it can claim that the processing relies on one of the criteria established by the law.[54] The set of criteria is exhaustive, so that if a data controller is unable to rely on one of them the processing is unlawful. Financial data are considered of non-sensitive nature.[55]

For Open Finance, the relevant legal bases for a legitimate processing under Article 6 GDPR are in principle that the data subject has unambiguously given consent or that the data processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract. The complications surrounding the choice between the two legal bases will be discussed in the next Section.

Moreover, in the case at study fintech solutions make an extensive use of profiling techniques which constitute the business model. Where profiling occurs, the GDPR requires for an additional layer of

[52] See also Recital 90 PSD2.

[53] See Art. 5 GDPR, in particular where it states "personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (purpose limitation) and "personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (data minimisation).

[54] Art. 6 GDPR.

[55] This is so as they are not included in the exhaustive list of sensitive data of Art. 9(1) GDPR.

control. It postulates that individuals have the right not to be subject to a decision based solely on automated processing to evaluate certain personal aspects of a person.[56] Profiling can be used if it is necessary for contractual necessity, it is authorised by EU or national law, or it is based on the data subject's 'explicit consent'. In the case of automated decisions based on 'explicit consent' or contractual fulfilment, controllers must respect a right for data subjects to obtain human intervention, express their point of view, and contest decisions.[57]

Another important provision of the GDPR to empower data subjects is the right to data portability, i.e. their right to transmit or have the data transmitted to another controller where the processing is based on the legal bases of 'consent' or on a contract.[58] Consent and contract necessity are only two of the grounds for lawful data processing as per Article 6 GDPR. The processing grounds of compliance with a legal obligation, protection of vital interests, the performance of a task carried out in the public interest, and the pursuit of legitimate interests of data controllers or third parties are therefore excluded from the data portability right. This narrow scope of the right is further restricted to data which data subjects have provided themselves to the data controller—so-called volunteered data. The scope of the provision includes active observation of the data but excludes derived or inferred data, or anything resulting from the analysis of the data.[59]

From these norms of the GDPR related to the PSD2 model, it emerges that in principle the two laws are not necessarily in conflict - as it may have *prima facie* appeared – since they both aim to grant transparency and user control.

However, inconsistencies arise from their cohabitation and coordination, starting from the legal basis legitimising the use of relevant financial data and the ensuing rights and obligations of the parties.

The leitmotiv of 'consent' in the two laws has already triggered discussions and uncertainties within Member States and stakeholders regarding the correct implementation of the PSD2, especially in relation to measures concerning the protection of personal data.[60]

As far as data protection is concerned, Article 94(2) PSD2 stipulates that "payment service providers shall only *access*, *process and retain* personal data necessary for the provision of their payment services, with the *explicit consent* of the payment service user" (emphasis added). Moreover, other

[56] Art. 4(4) GDPR.
[57] Art. 22 GDPR.
[58] Art. 20 GDPR.
[59] Article 29 Working Party, 'Guidelines on the right to data portability' (Adopted on 13 December 2016, last Revised and adopted on 5 April 2017).
[60] See e.g. European Data Protection Board, *Letter to Sophie in 't Veld, Member of the European Parliament* (Brussels, 5 July 2018); BEUC, *Consumer-Friendly Open Banking* (Brussels, 20 September 2018); European Banking Federation, *European Banking Federation's comments on the Article 29 Working Party guidelines on consent* (wp259), (Brussels, 23 January 2018).

provisions of the PSD2 refer to 'consent' as regards authorisation of a payment transaction. Under Article 64 PSD2 "a payment transaction is considered to be authorised only if the payer has given *consent to execute the payment transaction*" (emphasis added). This 'consent' to authorise a payment is later referred as 'explicit consent' in Articles 65 and 66 PSD2 when specifying the actions that banks need to perform to ensure the payer's right to use a Payment Initiation Service[61] or an Account Information Service. Arguably, the 'consent' referred in these provisions do not relate to access or processing of data but to the authorisation of a service. It signifies contractual agreement albeit equivocally normed as 'explicit consent' in the realm of contract law.

4.2.The proposal for a Data Act

In the thrust towards innovation and competition, the European Commission has recently unveiled a proposal for a Regulation on fair access to and use of data, the so-called 'Data Act' (or 'Proposal')[62] pursuant to the European strategy for data.[63]

The Proposal addresses market concentration and it has the aim of ensuring fairness in the allocation of value from data and foster access to and use of data, creating a horizontal cross-sectoral governance framework. To achieve its goal, it ensures that a wider range of stakeholders gain availability of more data for innovative uses.

Of relevance here are the generalised rules on making data generated using a product or service mandatorily available to their users.[64] Products shall be created, and services provided, in such a manner that by default data generated by their use are easily, securely and directly accessible to the users.[65] When users wish to transfer these data to other providers, the data holders need to ensure that the data are shared transparently in fair, reasonable and non-discriminatory conditions.[66] To do so, the Proposal prohibits unfair contracts relating to data-related obligations and introduces a new unfairness test to protect weaker commercial parties such as SMEs.[67] The sharing may occur only upon request by users.[68] This requirement accords to them a portability right, extending the portability right already conferred to data subjects by Article 20 GDPR (above). This new extended portability right grants users the right to access and make available to third parties to any data irrespective of

[61] Art. 66 PSD2.
[62] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM/2022/68 final.
[63] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, COM/2020/66 final.
[64] Art 1 Data Act.
[65] Art 3 Data Act.
[66] Art 8 Data Act.
[67] Art 13 Data Act.
[68] Art 5 Data Act.

their nature as personal or non-personal, of the distinction between 'actually provided' or 'passively observed' data, and of the limited legal basis of the processing under Article 20 GDPR. Moreover, unlike the GDPR that reduces the reach of the right by providing that controllers may transfer data where it is 'technically feasible', the Proposal mandates such a technical feasibility.[69]

As a horizontal proposal, the Data Act envisages the above basic rules for all sectors as regards the rights to use data, but it leaves to vertical legislation the establishment of more detailed rules for the achievement of sector-specific regulatory objectives. For Open Finance, therefore, it will not yet introduce new data access rights in the financial sector, but it hints at a subsequent legislative vertical initiative aligned with the horizontal principles provided by the Data Act.[70] The anticipated review of the PSD2[71] and future framework for Open Finance would need to converge with the horizontal rules of the Data Act, provided that the latter will be confirmed through the EU legislative process.

In any event, the provisions of the Data Act on the binding nature of data transfer clearly generalise the mandatory data sharing already adopted by the PSD2 upon consent of the customer.

As a consumer-centric initiative focusing on consumer empowerment, therefore, the key questions remain whether the PSD2 model and the Data Act are robust enough for consumer protection beyond the alleged benefits of Open Finance, and what the risks for consumers are.

4.3.The approach in the United Kingdom

While in the EU the PSD2 enabled Open Banking contemplating both retail and corporate banks, in the UK the Competition and Market Authority ('CMA') launched it by first mandating to the country's nine largest banks only to open to TPP regulated by the Financial Conduct Authority ('FCA'), and providing standardised rules subject to the consent of their customers.[72] Through this experience it has led the public debate on Open Finance and the set-up of an advisory group to drive forward the strategy for its implementation.[73]

The UK approach is grounded on principles and conduct of business rules, where the latter are best seen to adapt to the specific mechanisms of Open Finance.

---

[69] Art.5 See also Recital 31 Data Act.

[70] Data Act, explanatory memorandum p. 5.

[71] European Commission, Consultation Document Targeted Consultation on the Review of the Revised Payment Services Directive PSD2,(2022), available at https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en.

[72] Competition and Market Authority, Retail Banking Market Investigation Order 2017, available at https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf.

[73] Financial Conduct Authority, Business Plan 2019/20 (2019), available at https://www.fca.org.uk/publication/business-plans/business-plan-2019-20.pdf; Financial Conduct Authority, Advisory Group on open finance, available at https://www.fca.org.uk/firms/advisory-group-open-finance.

In the draft principles of Open Finance, it has been set out that regulation would be needed to ensure that consumers are protected, data is used ethically and in a way that they have consented to and expect, and that liability is clear and effective redress ensured when problems occur.

To achieve the goals, the debate focuses on TPPs being authorised and held to appropriate standards. They should be subject to appropriate threshold conditions on financial resources, appropriate systems and controls, operational resilience requirements and security architecture. Regulation of TPPs and their activities emerges in the public debate to ensure consumers do not face a patchwork of regulated and unregulated activities, which could also help ensure that consumers have access to the Financial Ombudsman Service when needed. Concerns are express with regard to the UK data protection legislation. Accordingly, the UK GDPR is not considered to be designed and adequate to support a full Open Finance framework. Therefore, any new regulation needs to work with UK GDPR.[74] The Information Commissioner's Office (ICO) itself agrees that the UK GDPR applies to the

general process of personal data rather than providing for any specific sector. To the extent that the UK GDPR proves insufficient, therefore, the approach is that any additional regulation should be focused on the specific mechanisms of Open Finance.[75]

Hence, the general theme in the UK differs from the EU debate in that the experience of Open Banking should be the starting point in terms of liability, data rights, standards and ethics. At the same time, however, the specific risks in each financial sector should be considered and integrated in the regulation of Open Finance. From this perspective, additional layers of consumer protection are needed in the form of conduct of business rules.

5. Open Risks

5.1.Legal uncertainty and the lack of effective control

As noted, Open Finance is meant to be customer-centric and rest on consumers' control of the data. It is therefore essential to determine what is the legal basis for data processing, and how consumers are empowered and remain effectively in control.

[74] Financial Conduct Authority, Open Finance, Feedback Statement FS21/7 (March 2021) available at https://www.fca.org.uk/publication/feedback/fs21-7.pdf

[75] https://ico.org.uk/media/about-the-ico/consultation-responses/2617565/ico-response-fca-open-finance-20200313.pdf

Under the PSD2 it is already unclear whether the processing of account data finds its legal basis in the contractual necessity under Article 6(1)(b) GDPR or though the consent of the customer under Article 6(1)(a) GDPR.

Article 94(2) PSD2, under Chapter 4 titled "data protection", stipulates that "payment service providers shall only *access*, *process and retain* personal data necessary for the provision of their payment services, with the *explicit consent* of the payment service user" (emphasis added). In so doing, the PSD2 seems to qualify the basis for processing account data with 'explicit consent'. However, the EDPB in a letter addressed to a European Member of Parliament (i.e. not laid down in the form of official guidelines) considers the 'explicit consent' of Article 94(2) PSD2 as contractual consent, thus not interfering with contractual necessity. According to the Authority,

> "article 94(2) of PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under PSD2, data subjects must be made fully aware of the purposes for which their personal data will be processed and have to explicitly agree to these clauses. *Such clauses should be clearly distinguishable from the other matters dealt with in the contract* and would need to be *explicitly accepted by the data subject*. The concept of explicit consent under Article 94(2) of PSD2 is therefore *an additional requirement of a contractual nature and is therefore not the same as (explicit) consent under the GDPR*"[76] (emphasis added).

Arguably, holding the 'explicit consent' as contractual would not explain why it has been expressed in the norm addressing data protection under a separate dedicated heading of the PSD2. In addition, this interpretation not only would dispute the letter of the norm where it affirms that 'explicit consent' is required for the access, processing and retention only to the extent necessary for the provision of the services, but it would also overlap with the contractual meaning of 'consent' used in Articles 64-67 PSD2. These other provisions of the PSD2 refer to 'consent' as regards authorisation of a payment transaction. Under Article 64 PSD2 "a payment transaction is considered to be authorised only if the payer has given *consent to execute the payment transaction*" (emphasis added). This simple 'consent' to authorise a payment is later referred as 'explicit consent' in Articles 65 and 66 PSD2 when specifying the actions that banks need to perform to ensure the payer's right to use a PIS.[77] Equally, AIS "shall provide services only where based on the payment service user's *explicit consent*".[78]

[76] European Data Protection Board, *Letter to Sophie in 't Veld, Member of the European Parliament* (Brussels, 5 July 2018).
[77] Art. 66 PSD2.
[78] Art. 67 PSD2.

(emphasis added). The 'consent' and 'explicit consent' referred in these provisions do not relate to access or processing of data but to the authorisation of a PIS or AIS service. It signifies contractual agreement albeit equivocally normed in the 'simple' versus 'explicit' dichotomy in the realm of contract law.

Likewise, the Data Act is silent on the legal basis for data processing, referring to a "request" by the user.[79] Where such user is not a data subject, the Data Act makes express reference to "a valid legal basis under Article 6(1)" of the GDPR.[80] True, the Data Act is meant to complement and be without prejudice to the GDPR,[81] although it would be clearer and desirable if it explicitly and unequivocally specified that in case of conflict between the two the provisions of the GDPR should prevail.[82]
At any rate, the legal uncertainty over the use of 'consent' or 'contractual necessity' remains. Either way, moreover, both legal bases for data processing could be problematic to ensure consumer control in an Open Finance ecosystem.

5.1.1. Contractual necessity ex Article 6(1)(b) GDPR

The legal basis of contractual necessity needs to be considered in the context of the obligations of purpose limitation and data minimisation laid down by the GDPR. Data needs to be as little as possible and they must be collected for specified, explicit and legitimate purposes. They should not be further processed in a manner that is incompatible with the initial purposes.[83] These requirements already pose some problems as to their suitability with Open Finance, since the data were originally collected under a different set of contracts in different product lines.
At any rate, data processing must be objectively "necessary" for the performance of the contract or for taking steps prior to entering into a contract. It is established case-law that the requirement of 'necessity' does not equates to what is permitted by or written into the terms of a contract, especially consumer contracts that typically are not negotiated on an individual basis.[84] Instead, the assessment needs to be fact-based vis-à-vis the objective pursued. If there are other realistic less intrusive alternatives the processing is not necessary. Therefore, it does not include processing which is useful but not objectively necessary.[85]

[79] Articles 4 and 5 Data Act; Recital 31 Data Act.
[80] Article 4 Data Act.
[81] Article 1(3) Data Act; Recital 7 Data Act.
[82] This is to avoid risks of interpretation regarding e.g. the special law vs general law or posterior vs anterior law relationship between the two. See also EDPB-EDPS, Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act), (4 May 2022), p 10.
[83] Article 5(1)(b) and (c).
[84] Case *Heinz Huber v Bundesrepublik Deutschland* (C-524/06) ECLI:EU:C:2008:724.
[85] Joined cases *Volker und Markus Schecke GbR* (C-92/09) and *Hartmut Eifert* (C-93/09) *v Land Hessen* ECLI:EU:C:2010:662.

Contractual necessity must be interpreted strictly with particular regard to the aim, purpose or objective of the product or service. A controller needs to be able to demonstrate how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed without the processing.[86] Moreover, where contracts consist of separate services or options that can be performed independently of one another, the applicability of contractual necessity needs to be assessed in the context of each of those services or options separately.[87] Crucially, if a processing is necessary for the controller's business model but not for the strict provision of the service, the requirement of contractual necessity cannot be satisfied but other legal bases must be used.[88]

Within the Open Finance ecosystem in particular, and with big data generally, all data would become 'necessary' but it is doubtful the extent to which such a necessity is for the objective delivery of the service rather than the providers' business models. Arguably, the boundaries are blurred but the suspicion is that in many cases the processing leans more towards the satisfaction of the needs of new business models. In most instances, the primary roles and functions of financial services remain the same, but the way they are undertaken is changing —payments still need to be made, loans granted, savings and investments made, etc. Those specific activities still need to be undertaken as ever and do not change. What changes is how these activities are carried out and the roles undertaken by the providers. Moreover, it has to be reminded that most of the data processing for the provision of Open Finance services rests on correlations, not on causation.

Arguably, in conclusion, contractual necessity may be a lawful basis for processing on occasions to be verified case-by-case but hardly as the one of general applicability.

5.1.2. Consent ex Article 6(1)(a) GDPR

Consent under the GDPR is probably one of the most complicated lawful bases to implement,[89] and the addition of Article 94(2) PSD2 does not help.

As conceived by data protection law, it is a key element that permits the processing of personal data by data controllers that would otherwise be forbidden. When a data subject gives valid consent, data

[86] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (16 October 2019).
[87] *Ibid* p. 11.
[88] *Ibid*.
[89] Exemplified by the many interpretative interventions of the supervisory authority for data protection, the European Data Protection Board – 'EDPB' (formerly, Article 29 Working Party): Article 29 Working Party, *Opinion 15/2011 on the Definition of Consent*, 01197/11/ENWP187 (July 13, 2011); Article 29 Working Party, *Article 29 Working Party Guidelines on consent under Regulation 2016/679* (Adopted on 28 November 2017, and last Revised and adopted on 10 April 2018); European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* (Brussels, 4 May 2020).

controllers are released from the restrictions provided by law. The processing becomes lawful from the moment consent is unambiguously expressed.

By law, consent shall be granular and distinguished from declarations concerning other matters (Article 7[2] GDPR). It must be "freely given, specific, informed and unambiguous" (Article 4[11] GDPR). Correspondingly, the law mandates 'affirmative consent' requiring the data subject to signal agreement by "a statement or a clear affirmative action" (Article 4[11] GDPR). At the same time, it continues to distinguish between 'explicit consent' if the data in question is sensitive personal data, and 'unambiguous' consent for all the other personal data (Article 6 GDPR combined with Article 4 GDPR).

The issue of what standard of consent should apply under the GDPR was the subject-matter of intense debates and negotiations at the lengthy proposal stage of the GDPR. The legislative history of the GDPR demonstrates that the final drafting was intentional in maintaining different qualifiers of consent and making the express distinction between 'unambiguous' and 'explicit' consent depending on the ordinary or sensitive nature of the data. To the extent that the GDPR makes clear that 'explicit' and 'unambiguous' consent are not the same, the boundaries of what is 'unambiguous' remain unclear, with the additional complication that the law states that it must be given by an 'affirmative action'. For example, it is unclear to what extent implied consent remains possible.[90] While the GDPR provides that "silence, pre-ticked boxes or inactivity should not *(omissis)* constitute consent" (Recital 32 GDPR), it also states that consent can be given through "another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data" (Recital 32 GDPR). In any event, controllers must be able to demonstrate that data subjects have consented (Article 7 GDPR).

The distinction between 'explicit' and 'unambiguous' consent matters in practice as long as different models of consent translate into very different engineered solutions within financial products and services, especially online. In the 'explicit' consent model an opt-in tick box or declaratory consent statement will be necessary. However, in the 'unambiguous' consent model that dominates commercial services a prominent notice together with an 'affirmative action' may suffice to obtain an implied consent without the need for an opt-in box or declaratory consent.

In the consumer protection realm, this can make a substantial difference in terms of the way consent is collected from consumers or the interface presented to them, and the way in which they interact with the product or service provider.

[90] In this regard, the latest 2020 opinion of the EDPB does not help much, limiting their interpretation to "all presumed consents that were based on a more implied form of action by the data subject (e.g. a pre-ticked opt-in box) will also not be apt to the GDPR standard of consent". See European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (Brussels, 4 May 2020), 20.

Ultimately, this also makes a difference as to the real knowledge and control that consumers may have on the processing of their personal data, and the uses that can be made with the data. Consent must rely on transparency and an 'affirmative action' (whether explicitly given or inferred through conduct) but how this translates in practice remains vague, especially in the context of Open Finance and within the complexities of financial transactions.

It needs to be added that the GDPR establishes explicitly that data subjects have a subsequent right of withdrawal of consent. The data subject may withdraw consent at any time and this must be as practical as granting consent. Clearly, however, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (Art. 7(3) GDPR).

The complexities of the Fintech business models, data-collection practices, vendor-customer relationships, or technological applications may make it impossible for consumers to understand what they are consenting. Equally, these complexities may in practice render consumers unable to freely and actively decide to accept the consequences of consenting to data processing, particularly when faced with a perceived immediate economic benefit.

Despite the apparently robust legal protection afforded to data subjects, consent may be obtained by a number of methods and has proved problematic as a basis for data processing because it can be easily abused, confused, or conflated.[91]

Treating consent as a transactional moment using standard form agreements may constitute a mechanical or perfunctory means of obtaining overarching consent for data processing.[92]

For instance, the condition of consent in the provision of financial services is a common yet elusive method of obtaining consumer consent. Consent becomes associated with the legal paradigm of contract. At the same time, the contractual relationship is a situation with a typical imbalance between the consumer and the business counterpart. Consumers are presented with no much choice but to abide by the lenders' terms if they wish to receive a service. In practice, the consumer's consent becomes either mandatory or assumed. Open Finance is based on data exploitation. As seen above, the PSD2 names contractual consent and data processing consent in the same way ('explicit consent'), albeit in two different Articles and contexts.[93]

---

[91] In theory, consent that does not meet the requirements of the law or is vitiated should be regarded as void, and should invalidate all data processing *ex tunc*—from the outset. See Article 29 Working Party, Article 29 Working Party Guidelines on consent under Regulation 2016/679 (Adopted on 28 November 2017, and last Revised and adopted on 10 April 2018). For specific literature see e.g. MANTELERO A, "The future of consumer data protection in the EU. Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics" 30 *Computer Law and Security Review* (2014), 643-660; KOSTA E, *Consent in European Data Protection Law* (Martinus Nijhoff, 2013).

[92] BROWNSWORD R, "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality", in Gutwirth S et al. (eds.) *Reinventing Data Protection?* (Springer, 2009), 83-110.

[93] Articles 64-67 PSD2 and Article 94 PSD2.

The legal mechanism of consent becomes more confused where the GDPR further intends to protect data subjects stating that 'consent' should not be regarded as freely given if they are "unable to refuse or withdraw consent without detriment" (Recital 42 GDPR) or "where there is a clear imbalance between the data subject and the controller" (Recital 43 GDPR). Recent studies show that in order to gain specific transactional and personal advantages most consumers willingly consent or disclose information about themselves and their social activities without thinking about the effects of their disclosures, thus making consent *de facto* ineffective. Yet very few consumers understand the significant consequences of this trade-off, including how data controllers use their personal data. Not only data processing can be very complex and non-transparent, but most consumers lack both the information and the skills to properly evaluate their own decision to consent.[94]

In the end, under the discussed legal uncertainties it remains unclear how the aspirations of placing consumers in control can be effectively reconciled with the reality of Open Finance.

5.2.Black boxes and dark patterns

It has to be reminded that the expanded data processing is mostly done in the interest of the financial services industry to enlarge the customer base, minimise risks, and increase profitability. True, these elements may coincide with product innovation. At the same time, these interests may not necessarily coincide with the provision of suitable products in the interest of consumers in terms of provision of financial services at affordable costs to those who really need and qualify for them.

Open Finance relies on enhanced data sharing for personalisation and profiling purposes. Personalisation relies on profiling. The latter is about prediction, which is not the same as knowledge. Unlike knowledge, it is not neutral and it is used to determine the future. Therefore, the risk is that Open Finance will create a more complex and fragmented financial environment where data analytics may exploit or manipulate consumer behaviour or biases.

The problem is that these systems are overly complex, not transparent and there are no mechanisms to safeguard against abuses and mistakes – generally known as the 'black box' problem.[95]

---

[94] PASQUALE F, *The Black Box Society* (Harvard University Press, 2015); PEPPET SR, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future", 105(3) *Northwestern University Law Review* (2011), 1153-1204; BORGHI M, FERRETTI F, and KARAPAPA S, "Online Data Processing Consent Under EU Law: A Theoretical Framework and Empirical Evidence from the UK", 21 *International Journal of Law and Information Technology* (2013), 109 – 153; EDGAR A, WHITLEY A, and PUJADAS R, "Report on a study of how consumers currently consent to share their financial data with a third party", *Report provided for the Financial Services Consumer Panel* (London, 19 April 2018), at https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf.

[95] PASQUALE, *supra* note 94.

Most of the time not only the logics/biases of the algorithms remain undisclosed and guarded as trade secrets, but also the data sources used by the individual lenders are undisclosed. Arguably, it is very difficult to determine how the data are correlated and whether the variety of unrelated data operate as proxies for personal features – also of sensitive nature – targeting vulnerable individuals or behavioural biases. The issue of selecting qualitative in addition to quantitative data can pose the risk of unintentional or even intentional discrimination (e.g. by cherry-picking certain customers to increase profitability), especially since their choice reflect biased human decisions in the design of the algorithm, and thus of the product or service. Algorithms work on the basis of predetermined features or variables. Therefore, they are in a sense inherently biased or discriminatory. They assess the features of a person – thus his/her viability - according to the behaviour of others. In this way, the most appropriately designed algorithm is the one that can select, or discriminate, most effectively or better than others. This is a fundamental feature of algorithms that cannot be avoided. Obviously, the resulting products or services do not overtly discriminate on the basis of factors such as race, gender or age that are caught by anti-discrimination laws.[96] Nevertheless, they may instead use correlated information to build an in-depth profile of a particular customer and make indirect or other discriminations not explicitly covered by the law, e.g. discriminations based on behaviours, culture or wealth. Some instances of these discriminations can be re-conduced to traits of race, gender, or age but they will be very hard - if not impossible - to prove. Big data may dig-up protected information.

An indiscriminate use of data may easily lead to increased stereotypical decisions. They may respond to schemes selecting certain groups of the population posing issues of access to financial services to those groups of consumers.

In this environment, the risk of dark patterns is concrete. Dark patterns are "business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They *(...)* are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances".[97]

[96] E.g. see Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180/22; Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, OJ L 373/37. See also *Association Belge des Consommateurs Test-Achats ASBL and Others v Conseil des ministers* (Case C-236/09), ECLI:EU:C:2011:100, where the CJEU ruled that insurers can no longer take gender into account when calculating insurance premiums.

[97] OECD, "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336 (OECD Publishing 2022), https://doi.org/10.1787/44f5e846-en

The subversion or impairment of consumer autonomy is the contrary of a consumer-centric environment and effective control. A critical point is that of attempting to empower consumers in an environment of vulnerability to dark patterns and other online perils.[98]

The Data Act attempts to fix the problem. It provides that third parties shall not "coerce, deceive or manipulate the user in any way" by subverting or impairing their autonomy, decision-making or choices, including by means of a digital interface.[99] However, it does not explicitly rule the prohibition of any form of coercion, deception or manipulation of data subjects, regardless of whether the user is also a data subject.[100] Under the Data Act, 'users' are natural or legal persons that own, rent or lease a product or receive a service.[101] The factors that may affect decision-making - hence real control of the data - may be different depending on whether or not the 'user' is also the data subject.[102]

The above difficulties could have additional counterproductive effects if a number of consumers become untrustworthy of their data being processed properly. Sections of the population may become averse to share information for fear of having their personal integrity violated. This, in a vicious circle, poses challenges to the commercial use of the data that will leave them behind or excluded.

On a related line, there are risks for those segments of the population who are un-networked or have no or limited digital presence. With Fintech development, increasing concerns are expressed by groups of consumers who face difficulties to access information, or buy and pay for goods/services in the digital domain. These include elderly persons who for various reasons do not use technologies, persons with disabilities, or persons in poverty. The causes for these difficulties may be diverse and range from a lack of digital literacy, lack of accessibility to the digital devices supporting the financial services, as well as lack of trust in digitalised services (e.g. fear around fraudulent use of identity, difficulty to identify misuse and claim redress, etc.).[103] The problems of consumer vulnerability in the digital sphere are well documented in the literature,[104] with the addition of the other layer of

[98] *Ibid.* See also SEIZOV O, WULF A and LUZAK J*,* "The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU**"**, 42 *Journal of Consumer Policy*, 2019, 149-173.
[99] Article 6(2)(a) Data Act.
[100] EDPB-EDPS, *supra* note 82.
[101] Article 2(5) Data Act.
[102] EDPB-EDPS, *supra* note 82.
[103] OECD, *G20/OECD INFE Report on Ensuring Financial Education and Consumer Protection in the Digital Age* (2017); Central Bank of Ireland, *Discussion Paper: Consumer Protection Code and the Digitalisation of Financial Services* (June 2017).
[104] For all, see Helberger N, Sax M, Strycharz J Micklitz H, "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability", 45 *Journal of Consumer Policy* (2022), 175, and the literature there cited. See also ALPA G and CARTICALA' A, *Diritto dei Consumatori* (Il Mulino, 2016).

vulnerability in the realm of financial services.[105] As a result, significant numbers of consumers could be denied access to financial services.

In any event, the concern may not be limited to those who are not digitalised. The broader question, affecting everyone, is the extent to which people remain with the liberty of being un-networked or offline, with the safeguard of not attracting negative consequences in case personal data are not available digitally or refusal to share data.[106]

All in all, these risks raise debates and concerns over the commodification of personal data, the financialisation of people's lives, and the shaping and conforming of behaviours beyond the provision of financial services. These issues have not been discussed sufficiently in the making of the PSD2 or the Data Act.

6. Conclusions

This work was concerned with Open Finance and the challenges facing EU regulation to adequately protect consumers. Following the opportunities provided by Open Banking via the PSD2, the EU aims to extend this data-driven financial model to the entire financial services sector.

To enable Open Finance, regulation is needed. The question is what kind of regulation. The EU places consumer empowerment and data control as the tools to achieve a consumer-centric data-driven financial market led by innovation. How factual consumer empowerment, data control and protection can be reconciled with the regulatory approach currently envisaged by the EU legislator is an open matter that raises doubts and needs to be carefully addressed.

The regulatory framework for Open Finance rests in the consolidation and extension of a sectoral PSD2-like legislation that will have to integrate the general framework provided by the proposed Data Act. Moreover, as personal data are involved, it overlaps and needs coordination with the GDPR.

An analysis of the current and proposed EU legal instruments to enable Open Finance reveals that the latter may rather open risks for consumer protection for providing legal uncertainty and failing to grant an environment where consumers are indeed in control and find adequate protection. Black boxes and dark patterns may flourish in such an environment. In a financial services market that is mainly supply-driven and governed by the supply-side, there are conduct of business risks.

[105] PAGLIETTI M and RABITTI M, "A Matter of Time. Digital-Financial Consumers' Vulnerability in the Retail Payments Market", 33(4) *European Business Law Review* (2022), 581.

[106] PACKIN G and ARETZ L, "On Social Credit and the Right to Be Unnetworked", 2 *Columbia Business Law Review* (2016), 339.

Aggressive business models may expand via the digital development. Innovation and competition are welcome, but data-driven business models are complex and take new unconventional forms where data feed new scenarios and create new markets. This can result in an environment favourable for targeted individual marketing, exploitation of consumers' behavioural biases, mis-selling of financial services, or financial discrimination. Freeriding wallows in legal uncertainty and may flourish.

The identified risks stemming from Open Finance may derive from the failure of the approach taken by present and proposed regulation to deliver the goal of realistically placing consumers at the centre and put them in control. Such a goal could not happen with the usual legal instruments of consumer consent or reliance on contractual necessity for data processing. This is particularly the case already in a context of the legal uncertainty over their use in the PSD2 as the proper legal basis under the GDPR.

More than in any other market, in the digital environment vulnerability is likely to be the norm rather than the exception.[107] In Open Finance, consumers face the combination of both digital and financial vulnerability. Arguably, there is a need for a paradigm shift reversing the expectations placed on consumers to be self-governing and the arbiters of markets, particularly the digital financial one. In vulnerability-sensitive markets data control should be by regulatory and technological design, and not left to the autonomy of consumers. The use of principles integrated by conduct of business rules is the leading debate taking place in neighbouring jurisdictions such as the UK.

Consumer protection concerns intensify if regulation aims to achieve autonomy through the instrument of consent. Digitalisation exacerbates the weaknesses of this legal technique designed to empower consumers. In addition, consumers are likely to consent too easily when faced with perceived immediate financial gains.

Thus, the overarching question is the extent to which the current regulatory approach taken by the EU is prone to sufficiently protect consumers from the fundamental problems likely to be opened by Open Finance.

All the above considerations need to go along with ever-existing problems of lack of effective supervision and enforcement in the digital domain – this is a theme that this paper has not addressed but that needs equal in-depth attention by complementing research.

[107] RIEFA C, "Protecting Vulnerable Consumers in the Digital Single Market", 33(4) *European Business Law Review* (2022), 607.