Forthcoming (2020) *Common Market Law Review*

THE EVOLUTION AND FUTURE OF DATA-DRIVEN FINANCE IN THE EU

DIRK ZETZSCHE,* DOUGLAS ARNER,* ROSS BUCKLEY,*** & ROLF WEBER****

Abstract

Europe's path to digitization and datafication in finance rests on four pillars: (1) extensive reporting requirements imposed after the global financial crisis to control systemic risk and change financial sector behaviour; (2) strict data protection rules reflecting European concerns about dominant actors in the data and technology industries; (3) the facilitation of open banking to enhance competition in banking and payments; and (4) systems for digital identification for individuals and legal entities designed to further the Single Market and enhance financial integrity and transparency. The article analyses these pillars and suggests that - together - they are triggering a transition to data-driven finance and will underpin the future of digital financial services in the EU. The pillars bolster an emerging ecosystem which aims to promote a balance among a range of sometimes conflicting objectives, including systemic risk, data security and privacy, efficiency, customer protection, and market integrity. As well as supporting digital financial transformation in Europe, the EU experiences provide important insights for other societies in developing regulatory approaches to the intersection of data, finance and technology.

KEYWORDS: Data Protection, Digital Identity, FinTech, Financial Regulation, General

---

* Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg, and Director, Centre for Business and Corporate Law, Heinrich-Heine-University, Düsseldorf, Germany.

** Kerry Holdings Professor in Law and Director, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong.

*** KPMG Law and King & Wood Mallesons Chair of Disruptive Innovation, Scientia Professor, and Member, Centre for Law, Markets and Regulation, UNSW Sydney.

**** Professor of Law emeritus, Co-Chair of Competence Center Financial Market Regulation, University of Zurich, Switzerland.

We would like to thank for support of this research the Australian Research Council as part of the project, "Regulating a Revolution: A New Regulatory Model for Digital Finance", the Hong Kong Research Grants Council Research Impact Fund and the Qatar National Research Fund National Priorities Research Programme as well as participants at the European Banking Institute annual conference in Frankfurt in February 2019, among many others around the world, for their comments and Pamela Cela, Tsany Ratna Dewi, Svea Pillard, Zak Vidor Staub and Robin Veidt for their most helpful research assistance. The article benefitted from thoughtful comments by two anonymous reviewers for which the authors are grateful.

Data Protection Regulation (GDPR), Open Banking, Payment Services Directive 2 (PSD II), RegTech, Single Financial Market.

JEL CLASSIFICATIONS: D23, G38, K22, L22, M15, O16.

1. Introduction

Some of the biggest questions facing societies today centre on the current and future roles of data, technology and regulation, in relation to finance and the digital economy, and more broadly. In this context, it is unsurprising that one of the major challenges facing the financial industry globally is the at times conflicting requirements of data regulation and financial regulation. The 2008 Global Financial Crisis led to an internationally coordinated process of regulatory reform, focused on reducing risk-taking and systemic risks in the financial sector.[1]

These reforms have caused substantial structural changes in finance around the world. They have also been a major driving factor in the adoption and use of data-driven technologies for compliance and regulatory purposes, today encompassed under the rubric of "regulatory technology" or RegTech.[2] At the same time, the General Data Protection Regulation (GDPR[3]) has introduced in the EU the world's most comprehensive system of data governance.

In this article, we argue that a combination of financial regulatory and data regulatory reforms in the EU are driving the rise of data-driven finance across Europe and transforming the Single Financial Market. Traditionally, banking and finance were seen as relational businesses and operated that way for centuries. A banking relationship commences when a potential customer enters a branch, asks to open an account, and then supplies the bank with the information it asks for, to be able to do so. With data-driven finance, the bank, or financial service provider, starts with the information it already has about the customer that it has acquired in the market, or gained in another role it may

---

[1]See e.g. Avgouleas, "Global financial crisis, behavioral finance and financial regulation: In search of a new orthodoxy", 9 *Journal of Corporate Law Studies* (2009), 23–59; Brummer, "Origins of the financial crisis and international/national responses: An overview", 104 *American Society of International Law Proceedings* (2010), 435–438; Moshirian, "The global financial crisis and the evolution of markets, institutions and regulation", 35 *Journal of Banking and Finance* (2011), 502–511; Buckley and Arner, *From Crisis to Crisis: The Global Financial System and Regulatory Failure* (Kluwer Law International, 2011).

[2]See Enriques, "Financial supervisors and Regtech: Four roles and four challenges", 53 *Revue Trimestrielle de Droit Financier* (2017) (detailing four different meanings of RegTech); Colaert, *RegTech as a Response to Regulatory Expansion in the Financial Sector*, Working Paper (June 2018), available at <ssrn.com/abstract=2677116> (last visited 6 Nov. 2019); Micheler and Whaley, "Regulatory technology: Replacing law with computer code", 20 EBOR (2019), 1–29 (analysing RegTech-based regulation); Arner, Barberis and Buckley, "FinTech, RegTech and the reconceptualisation of financial regulation", 37 *Northwestern Journal of International Law & Business* (2017), 371–414; Arner, Barberis and Buckley, "The emergence of Regtech 2.0: From know your customer to know your data", 44 *Journal of Financial Transformation* (2016), 79–86.

[3]See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, O.J. 2016, L 119/1.

play, such as a payments provider, and may then approach the customer armed with this data about them. Data-driven finance starts with a different perspective, and depends more heavily on the analysis of data in assessing credit and other factors – data which is relatively cheap – as compared to building a relationship and collecting information directly from the customer, which is expensive.

The interaction of four independent sets of reforms has not only established the framework for digital finance going forward, but – through the detailed requirements across this series of different initiatives – is directly driving the development of digital finance in the EU. While Europe has often been seen as lagging behind in this area, the acceleration of data-driven finance is rapidly transforming finance in the EU, with important implications for the Single Market and for other markets around the world. There is much to learn from an analysis of the EU's experience with regulating both finance and data, yet analysis of this intersection of data and financial regulation has so far been very limited.

In the following section we evaluate the origins of data-driven finance. In section 3, we argue that four seemingly unrelated EU regulatory frameworks introduced since the 2008 Global Financial Crisis, are together providing a regulatory ecosystem that is spurring the transformative transition from relationship-based to data-driven banking and finance. In section 4 we place European developments into context and discuss the steps required of intermediaries and regulators to build a fully developed approach to data-driven finance, based on an appropriately designed RegTech framework. Section 5 concludes.

2. The origins of digital finance

Financial technology (FinTech) is growing rapidly and creating new opportunities through – among others – big data,[4] the Internet of Things (IoT),[5] artificial intelligence (AI) and machine learning.[6] New infrastructure, such as distributed ledger technology and

[4]See Cohen, "What privacy is for", 126 *Harvard L. R.* (2013), 1904–1933; Barocas and Selbst, "Big data's disparate impact", 104 *California L. R.* (2016), 671–732; Katz, "Quantitative legal prediction – or – How I learned to stop worrying and start preparing for the data driven future of the legal services industry", 62 *Emory Law Journal* (2013), 909–966; Zetzsche, Buckley, Arner & Barberis, "From FinTech to TechFin: The regulatory challenges of data-driven finance", 14 *New York University Journal of Law & Business* (2018), 393.

[5]The IoT is a network of devices and applications containing software, electronics, actuators and connectivity that allows these things to connect, interact and exchange data; for an early general overview, see generally Weber and Weber, *Internet of Things: Legal Perspectives* (Springer, 2009).

[6]In computer science, AI research is defined as the study of devices that perceive their environment and take actions that maximize their chance of successfully achieving their task. The base line of artificial intelligence is a computer mimicking human "cognitive" functions such as "learning" and "problem solving". Artificial intelligence today can be used to detect unexpected correlations in large data pools, test expected correlations for causation or determine an empirical probability of a predefined pattern. See Poole, Mackworth and Goebel, *Computational Intelligence: A Logical Approach* (OUP, 1998), at p. 1; Russel and Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed., (Pearson, 2009).

blockchain,[7] enables the execution of transactions through smart contracts[8] and facilitates the establishment of digital identity,[9] together with many other use cases. Sometimes these innovations arise through regulatory arbitrage or regulatory avoidance; sometimes they are the direct result of the implementation of regulation.

In the financial markets a large variety of new business models have been developed. Examples include crowdfunding,[10] digital currencies,[11] initial coin offerings,[12] touchless and e-payment solutions[13] and robo advisors;[14] all these recently displayed forms of data-driven finance show the breadth of evolving FinTech applications.

Digital financial transformation has been a much longer process and has been taking place around the world since the early 1970s.[15] However, the speed of transformation has accelerated dramatically over the past decade, as technology and regulation have combined to drive the development of new models, new approaches and new players.

At the same time, rapid evolution in FinTech is raising new risks. The sheer amount of data facilitates looking at correlations rather than causations, and correlations can lead to unintended, and socially regressive, consequences. For instance, algorithms can discriminate wrongfully against certain groups of people: if data analytics show a certain race or gender generally has a better credit score, that better score could derive from existing biases against other races or genders, or the algorithm could be programmed to analyse data in a certain way that reflects biases existing among developer groups, or their clients, respectively.[16]

---

[7]See Rodrigues, "Law and the blockchain", 104 *Iowa Law Review* (2019), 679–729; Zetzsche, Buckley and Arner, "The distributed liability of distributed ledgers: Legal risks of blockchain", 4 *University of Illinois Law Review* (2018), 1361–1406.

[8]See Sklaroff, "Smart contracts and the cost of inflexibility", 166 *University of Pennsylvania Law Review* (2017), at 263; Werbach and Cornell, "Contracts ex machina", 67 *Duke Law Journal* (2017), at 313; Weber, "Smart contracts: Do we need new legal rules?" in De Franceschi, Schulze, Graziadei, Riente, Sica and Sirena (Eds.), *Digital Revolution – New Challenges for Law* (C.H. Beck, 2019), p. 299.

[9]See Arner, Zetzsche, Buckley and Barberis, "The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities", 20 EBOR (2019), 55–80.

[10]See Gutfleisch, "Crowdfunding and initial coin offerings under the EU legal framework", 15 *European Company Law Journal* (2018), at 73; Zetzsche and Preiner, "Cross-border crowdfunding towards a single crowdfunding market", 19 EBOR (2018), at 217.

[11]See Nabilou and Prüm, "Ignorance, debt and cryptocurrencies: The old and the new in the law and economics of concurrent currencies", 5 *Journal of Financial Regulation* (2019), at 1.

[12]See Cohney, Hoffman, Sklaroff and Wishnick, "Coin-operated capitalism", 119 *Columbia L. R.* (2019), at 591; dell'Erba, "Initial coin offerings: The response of regulatory authorities", 14 *New York University Journal of Law & Business* (2018), 1109 et seq.; Zetzsche, Buckley, Arner and Föhr, "The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators", 60 Harv. Int'l L.J. (2019), at 301.

[13]Maume, "In unchartered territory – Banking supervision meets Fintech", *Corporate Finance* (2017), at 272.

[14]See Ringe and Ruof, *A Regulatory Sandbox for Robo Advice*, EBI Working Paper Series 26/2018.

[15]See Arner, Barberis and Buckley, "The evolution of FinTech: A new post-crisis paradigm?" 47 GJIL (2016), at 1345; Brummer and Yadav, "Fintech and the innovation trilemma", 107 GJIL (2019), at 235 and 264.

[16]See e.g. Richardson, Schultz and Crawford, "Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice", 94 *New York University Law Review* (2019), at 192 and 204–217 (detailing examples of manipulated data in the criminal justice system, reflecting

Yet the methods to properly supervise and control self-learning algorithms are yet to be developed. Cybersecurity risks and tech-based complexity challenge supervisors and regulators trained to deal with traditional financial services.[17] The clash of cultures of traditional bankers and their lawyers communicating with computer scientists prompts risks of miscommunication and design and compliance failures. As a seemingly ever-increasing number of ever-more spectacular cyberattacks and IT bugs have demonstrated, these new risks could mean the net impact of FinTech for some market participants may be negative or even catastrophic.[18]

As finance evolves, so does its regulation. As developed in previous research, the new risks created by FinTech can be addressed by new approaches to regulation (which we have termed - in the FinTech context[19] - Smart Regulation[20]) paired with regulatory and supervisory technologies (collectively referred to as RegTech). RegTech describes the use of technology, particularly information technology (IT), for regulation, monitoring, reporting, compliance and systems design.[21] Examples include electronic Know-Your-Customer (KYC) systems which facilitate customer on-boarding by financial intermediaries and enhancement of market integrity,[22] automated compliance monitoring and reporting with regard to trading limits, and algorithm-based reviews of trading patterns in listed stocks, to ensure compliance with insider dealing laws.

FinTech and data-driven finance more generally lie at the intersection of finance, technology and regulation. At the heart of both FinTech and data-driven finance is the nexus of financial regulation and data regulation. This intersection, while challenging for regulators that need to deal with sometimes conflicting policy objectives, also provides an opportunity for us to conceptualize how regulatory systems are shaping the evolution of data-driven finance. This forms the subject of the second part of this article.

3. European developments in data-driven finance

Financial integration in Europe has evolved as a result of a series of major policy, legislative and regulatory strategies and initiatives, developed and implemented since the

---

racial bias). In the corporate context, see Enriques and Zetzsche, *Corporate Technologies and the Tech Nirvana Fallacy*, ECGI Law Working Paper 457/2019 (July 2019), at 31–34.

[17]See Arner, Zetzsche and Buckley, "FinTech, RegTech and systemic risk: The rise of global technology risk" in Arner, Avgouleas, Bush and Schwarcz (Eds.), *Systemic Risk in the Financial Sector: Ten Years after the Global Financial Crisis* (Centre for International Governance Innovation, 2019), pp. 69–82.

[18]Ibid.

[19]Unrelated to Fintech, the term has been introduced by Gunningham, Grabosky and Sinclair, *Smart Regulation: Designing Environmental Policy* (OUP, 1998). For an overview of that concept of Smart Regulation, see Gunningham and Sinclair, "Smart regulation" in Drahos (Ed.), *Regulatory Theory: Foundations and* applications (Anu Press, 2017).

[20]See Zetzsche, Buckley, Arner and Barberis, "Regulating a revolution: From regulatory sandboxes to smart regulation", 23 *Fordham Journal of Corporate and Financial Law* (2017), 31–103; see also Weber and Baisch, "FinTech – Eligible safeguards to foster the regulatory framework", 33 *Journal of International Banking Law and Regulation* (2018), 335-350.

[21]See Enriques, op. cit. *supra* note 2, *passim*; Micheler and Whaley, op. cit. *supra* note 2, at 6-8 (on the UK FCA's approach); Arner, Barberis and Buckley, op. cit. *supra* note 2, at 371; Weber, "RegTech as a new legal challenge", 46 *Journal of Financial Transformation* (2017), at 10.

[22]Arner, Zetzsche, Buckley and Barberis, op. cit. *supra* note 9, at 71-72.

1980s.[23] To name but a few, the European Economic and Monetary Union (EMU) and the Financial Services Action Plan in 1999[24] (with the 2001 Lamfalussy Report following shortly after),[25] the 2009 de Larosière Report in the aftermath of the 2008 Global Financial Crisis,[26] the Banking Union in the aftermath of the 2010 Eurozone Crisis[27] and most recently the pursuit of a Capital Markets Union (CMU),[28] with the European Commission's FinTech Action Plan of 2018 emerging from the CMU's mid-term review,[29] all have played central roles in supporting the development of the Single Financial Market on the basis of EU financial law.

Unlike the catalogue of previous strategic initiatives listed above, the disparate reforms culminating in 2018[30] were not designed to drive strategically the development, or digital financial transformation of, the Single Financial Market. The four legislative measures discussed here were all implemented for separate reasons, but their combined effect has been to give an extraordinary, unanticipated impetus to the digital transformation of finance in the EU, often requiring extensive use of RegTech by both industry participants and financial supervisors, and forming an iterative process rapidly moving the Single Financial Market towards data-driven finance. The specific measures were: extensiveness of digital regulatory reporting requirements (as part of a comprehensive process of post-Crisis financial regulatory reforms), the rigorous data protections of GDPR, the open banking regime introduced by the Payment Services Directive (PSD) II (particularly combined with the data portability requirements in the GDPR), and the pan-European digital identity framework based on the eIDASR and supplemented by the new anti-money laundering (AML) and other financial transparency and integrity reforms.

While outside observers have often not seen the EU as a leader in FinTech and digital financial transformation, we suggest that the EU's regulatory developments will have an important, long-term impact on the future development of data-driven finance in the EU and also around the world.

3.1. *Digitization of regulatory reporting*

---

[23]For the evolution of the EU Single Financial Market, the role of financial regulation and implications for global finance, see Avgouleas and Arner, "The Eurozone debt crisis and the European banking union: 'hard choices', 'intolerable dilemmas' and the question of sovereignty", 50 *The International Lawyer* (2017), 29–67, at 29; Arner and Buckley, "Redesigning the architecture of the global financial system", 11 *Melbourne Journal of International Law* (2010), 185–239, at 185; Weber and Arner, "Toward a new design for international financial regulation", 29 *University of Pennsylvania Journal of International Economic Law* (2007), 391–453, at 391.

[24]European Commission, Financial Services Action Plan, 1999.

[25]European Commission, The Final Report of the Committee of Wise Men on the Regulation of European Securities Markets, 15 Feb. 2001.

[26]High-Level Group on Financial Supervision in the EU, Report, 25 Feb. 2009.

[27]See Avgouleas and Arner, op. cit. *supra* note 23.

[28]See COM(2015)468 final, Action Plan on Building a Capital Markets Union, 30 Sept. 2015.

[29]See COM(2018)109 final, FinTech Action Plan: For a more competitive and innovative European financial sector, 8 Mar. 2018.

[30]The developments discussed in this article begin to emerge in the aftermath of the Global Financial Crisis of 2008, but reached their peak in or around 2018.

The first strand of change begins with financial regulation in the post-crisis environment. Since 2008, in tandem with post-crisis international regulatory approaches, European regulators have imposed very extensive reporting obligations on financial intermediaries in an effort to combat systemic risk and address a range of integrity risks emerging from money laundering, terrorism financing and competition scandals (in particular those around LIBOR and foreign exchange trading). Post-GFC changes included, *inter alia*, the Alternative Investment Fund Managers Directive (AIFMD 2011[31]), the European Markets Infrastructure Regulation (EMIR 2012[32]), and the recast Markets in Financial Instruments Directive (MiFID II[33]) adopted in 2014.

When MiFID II started to apply, in 2018, this brought global attention to the EU's requirements for digital financial reporting. However, MiFID II is merely one of a large number of EU financial regulatory reforms which have spurred rapid digitization of finance, financial reporting and regulatory capacity respecting digital finance. The most important regulatory initiatives in this regard include, for the banking sector the capital requirements instruments CRD IV[34]/CRR[35] (2013/2014), for the asset management sector the mentioned AIFMD (2011/2013), for financial markets the mentioned MiFID II and MiFIR[36] (2014/2018), for market infrastructure the European Market Infrastructure Regulation EMIR (2012/2013) and for payment services the PSD II (2015/2018).

These frameworks share a common focus on EU financial regulatory standards; and a common imposition of extensive reporting requirements on the financial services industry. Regulators in the EU, by requiring financial intermediaries to report large amounts of data on their decisions, activities and exposures, have triggered the digital financial transformation of Europe's regulated financial industry.

It is a given today that, when faced with a proposed legal instrument, the financial services industry will demand sufficient time to build the necessary IT systems to implement it. The necessity of technological implementation of regulatory reporting requirements has forced intermediaries and their service providers to continually invest in the development of their software and IT systems to ensure sufficient data is collected within their organization to meet reporting requirements, and that this data is packaged and reported in the necessary structure and form. This is the process of digitization. Digitization in turn makes possible the process of datafication: the application of computerized analytics tools to digital data. This is the second fundamental process of digital financial transformation and the gives the impulse for the evolution of data-driven finance in the traditional financial services industry. Digitization in the regulated financial

---

[31]See Directive, 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers, O.J. 2011, L 174/1.

[32]See Regulation (EU) 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, 27 July 2012, O.J. 2012, L 201/1–59.

[33]See Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments, O.J. 2014, L 173/349 (MiFID II).

[34]See Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, O.J. 2013, L 176/338.

[35]See Regulation (EU) 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms, O.J. 2013, L 176/1.

[36]See Regulation (EU) 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments, O.J. 2014, L 173/84.

services industry has made datafication both possible, but also necessary for a proper, comprehensive analysis of risks. Once financial intermediaries have digitized and datafied their reporting, regulators and supervisors are forced to develop data management systems capable of receiving and processing the volume of data being generated and delivered by the financial services industry. With enhanced analytics tools, supervisors can analyse even more data (and in turn, tend to ask the supervised entities to collect and transmit even more of it, triggering another RegTech cycle), which they increasingly request in the context of BCBS239 data aggregation requirements from the Basel Committee on Banking Supervision.

To give an example: when fund managers were required by the AIFMD in 2011 to report extensive data on investment strategies in a purely digital manner,[37] there was an outcry from small and middle-size firms arguing they would be disadvantaged relative to the large fund managers. Time has solved this problem. Eight years later, the data stream from fund managers via national competent authorities to the European Securities and Markets Authority (ESMA) flows smoothly. We expect the same for other regulatory initiatives if sufficient implementation time is granted - the latest example being the extensive reporting requirements introduced by MiFID II.

Perhaps the clearest example of digital financial transformation in the context of post-Crisis finance comes from an enforcement action against Merrill Lynch in October 2017 by the UK Financial Conduct Authority (FCA): the firm was fined just over GBP 34.5 million for failing to report some 68.5 million exchange traded derivatives transactions between 12 February 2014 and 6 February 2016,[38] as required under EMIR and MiFID.[39] From the standpoint of data-driven finance, the case highlights how the financial industry has been fully digitized and datafied: for how else could 68.5 million exchange traded transactions even occur, let alone be reported to regulators, over a two-year period, amounting to more than two transactions per second? Similar actions were concluded against other firms in 2019, including Goldman Sachs (GBP 34.3 million for failing to provide accurate and timely reporting relating to 220.2 million transaction reports) and UBS (GBP 27.6 million for failings relating to 135.8 million transaction reports).

Early results of the data streams to ESMA can now be seen: for instance, ESMA has produced and published comparative reports on fund fees[40] and financial instruments traded on European stock exchanges.[41]

Details of this development have been examined elsewhere.[42] What is clear is that the digitization of financial regulatory reporting is central to Europe's digital financial transformation, because this regulatory evolution has forced the financial services

---

[37]See Zetzsche and Eckner, "Investor information and reporting" in Zetzsche (Ed.), *The Alternative Investment Fund Directive*, 3rd ed. (Kluwer Law International, 2019).

[38]See FCA, "FCA fines Merrill Lynch £34.5 million for failing to report transactions", available at <fca.org.uk/news/press-releases/fca-fines-merrill-lynch-failing-report-transactions> (last visited 6 Nov. 2019).

[39]MiFID II has now extended these reporting requirements even further.

[40]See ESMA, *The Impact of Charges on Mutual Fund Returns* in Report on trends, risks and vulnerabilities, No. 2 (2017).

[41]See ESMA, *Financial Instruments Transparency System*, (2019).

[42]See Colaert, op. cit. *supra* note 2, *passim*; Micheler and Whaley, op. cit. *supra* note 2, at 6-17.

industry (and its regulators) to digitize data collection and regulatory reporting comprehensively, and moreover has provided the foundations for datafication. It is this combination – triggered by extensive post-Crisis financial regulatory reporting requirements under a wide range of EU legislation – that has accelerated the digital financial transformation of Europe's regulated financial services industry.

3.2. *Data protection and data governance*

The next strand of the process of digital financial transformation in the EU arises from the regulatory framework addressing data generally and its collection, use, storage and protection: the GDPR, implemented in 2018.

In the EU, Article 8(1) of the (indirectly via EU legal principles binding) ECHR, Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) TFEU together provide as a fundamental right and freedom that everyone has the right to the protection of their personal data. An extensive regulatory framework has developed around this right, with GDPR – replacing the first Data Protection Directive of 1995[43] – as the most significant evolution of this framework.

3.2.1. *GDPR's policy approach*

GDPR – covering all sectors of the economy – has imposed new data governance requirements upon the collection, use, storage and protection of data, with significant impact in the financial sector. As financial regulation drove the digitization of information in the financial industry, GDPR has driven spending on systems designed to appropriately manage that ever-increasing volume of data. Specifically, GDPR imposes rules that seek to protect natural persons in relation to the processing of their personal data,[44] excluding data relating to commercial entities.[45] GDPR is a response to the substantial increase in cross-border flows of personal data across the EU.[46] Based on the premise that trust is a crucial precondition for further developing the digital economy across the European internal market,[47] GDPR seeks to ensure a high level of protection of personal data. GDPR follows a technology neutral approach – it does not depend on the techniques used for data collection and processing, in order to prevent circumvention.[48]

The most important building block of the GDPR is that natural persons should have control of their own personal data. Under Article 6(1)(a), as set out in Recitals 40 and 42, the onus of proof that the data subject has given consent to the processing operation is on the data controller, i.e. the financial intermediary. According to Article 7(2) GDPR the request for consent must be presented in an intelligible and easily accessible form, using clear and plain language; consequently, general conditions might not suffice. Even where consent has been given, the circumstances under which consent

---

[43]See Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. 1995, L 281/31.
[44]GDPR, Recital 1.
[45]Ibid., Recital 18.
[46]Ibid., Recital 5.
[47]Ibid., Recital 7.
[48]Ibid., Recital 15.

has been achieved will be reviewed to remedy coercive pressure.[49]

In addition, data collected cannot be stored forever, but must be deleted in timeframes that relate to the objective for which the data was collected (data minimization principle). Following the *Google Spain* decision of the Court of Justice,[50] the GDPR further establishes a right to be forgotten upon request of the natural person, on a number of grounds, such as withdrawal of consent or where the data has been unlawfully processed.[51]

The approach embedded in the consent requirement is taken one step further with the data subject's right to data portability, stipulated in Article 20 GDPR: any natural person can ask the current data controller to transfer the data gathered, stored and processed to another controller in a structured, commonly used and machine-readable format. This approach is further reinforced, specifically for the banking industry, by PSD II's open banking provisions. GDPR likewise imposes portability across the entire economy, not only in the context of payments, a subject to which we will return.

In addition, GDPR contains a number of specific data organization requirements, including the pseudonymization of personal data, the use of online identifiers, and rules on tracing and profiling of users. In particular, natural persons have the right to be subject to a decision by humans (in contrast to a decision based solely on automated processing, including profiling) where the decision produces legal effects, such as entering or termination of a contract, or denial of rights.[52] Together with the "right to be forgotten" (which undermines the completeness of the data pool), the human decision requirement is targeting both the potentially undesirable impact of network effects and economies of scope and scale in data, and their tendency toward undesirable natural monopolies.

Responding to an intense debate among data protection experts, GDPR allows transfers of personal data to third countries or international organizations only in case of a positive adequacy decision, the existence of appropriate safeguards (in contractual relations), or the implementation of binding corporate rules (within corporate groups) pursuant to Articles 44 to 47 of GDPR.

The detailed provisions of the GDPR are paired with strong enforcement mechanisms. On the liability side, any person who has suffered material or non-material damage as a result of an infringement of the GDPR has a right to compensation from any controller or processor who was handling their personal data, even in the absence of contractual relationships between the person and the controller/processor.[53] At the same time, GDPR comes with heavy penalties, up to 4 percent of the total worldwide annual turnover of the corporate group to which the data controller or processor belongs.[54] The

---

[49]Ibid., Recital 42.

[50]See Case C-131/12, *Google Spain SL and Google Inc.* v. *Agencia Espanola de Proteccion de Datos (AEPD) and Mario Coteja Gonzales*, EU:C:2014:317; see also Weber, "On the search for an adequate scope of the right to be forgotten", 6 *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2015).

[51]See Art. 17(1) GDPR.

[52]See Art. 22(1) GDPR; three exemptions apply when the decision is a) necessary for entering into, or performance of, a contract between the data subject and a data controller, b) authorized by Union or Member State law, or c) is based on the data subject's explicit consent.

[53]See Art. 82(1) GDPR.

[54]See Art. 83 GDPR.

first year of GDPR practice, with some 60 sanctions proceedings, has left little doubt that the European data protection authorities are willing to impose sizeable penalties.[55]

3.2.2. *GDPR's impact on financial services*

In the context of European finance, GDPR's initial impact comes from its requiring financial intermediaries to reorganize their data processing and client data policies to meet the requirements of GDPR. The process of digitization combined with systemization to meet the requirements of GDPR has triggered a revolution in financial industry treatment of customer data, in the same way that MiFID II and its financial regulatory relatives have driven a revolution in financial industry collection and processing of business and regulatory data.

Financial intermediaries have often collected large amounts of data from and about their customers, over long periods of time. However, in many cases, this data has not been used effectively, because it has been restricted to certain business units, lines, products or silos within individual firms.[56] Financial intermediaries as a result of GDPR are now obliged to have comprehensive systems for their digitized data which address the collection, storage, use and protection of the data according to GDPR's requirements. The extensive details on personal data of individuals collected by many financial institutions also require data categorization tools which allow for amendments and deletion after a given timeframe or upon the natural person's request.

However – unlike the financial regulatory reforms which drive not only digitization but also datafication through the application of analytics to massive amounts of data – GDPR creates barriers to centralization of individual customer data and its use, placing requirements on the financial industry to develop new systems of data management and also shifting control of many aspects of their data from financial and data intermediaries (which have collected it) to individual customers (who are its subject).

Arguably, this may impair fully data-driven business models. For instance, financial institutions cannot contact new clients for distribution or sales purposes after acquisition of data pools from third parties unless the clients are legal persons only or the clients have consented *ex ante*, or the data pools were assembled through web-based gathering of user data.[57] Furthermore, data pools relating to the past become increasingly

---

[55]See Osborne, "Facebook could face $1.63bn fine under GDPR over latest data breach", *Zero Day*, 2 Oct. 2018, available at <zdnet.com/article/facebook-could-face-billions-in-fines-under-gdpr-over-latest-data-breach/> (last visited 6 Nov. 2019): the first high fine was imposed by the French Data Protection Authority in Jan. 2019, amounting to EUR 50 million on Google for not complying with the GDPR; Google has since filed a court complaint. Furthermore, it is estimated that Facebook could be fined up to USD 1.63 billion for its part in the Cambridge Analytica scandal.

[56]See Pereira da Silva and von Peter, "Financial instability: Can big data help connect the dots?" (Bank for International Settlements, 2018), available at <bis.org/speeches/sp181203.pdf> (last visited 6 Nov. 2019).

[57]The EU has introduced a specific data protection regime governing electronic communications, namely Directive 2002/58 that is planned, at the time of writing, to be replaced by a so-called E-Privacy Regulation. See Commission, COM(2017)10 final, Proposal for an ePrivacy Regulation. However, political objections, particularly in respect of the proposed cookies rules, have cast doubt on whether and when this Regulation will come into force; the last compromise draft dated October 2019 was rejected by 14 members of the EU Council Committee of Permanent Representatives in November 2019 [See CMS, "E-Privacy", available at <https://cms.law/en/deu/insight/e-privacy> (last visited 3 Feb. 2020)]. If the E-

unreliable for data analysis or risk management purposes to the extent that the GDPR's deletion requirements apply, removing partial benefits from the greater data gathering activity *ex ante*. These deficiencies could be considered and remedied in the risk models, for instance by adding further security margins to "old" or obviously deficient data pools, by mixing data from different sources, or applying filters. But all of this requires further sophistication in data gathering and processing methodology with potentially less competition arising from the greater concentration of data.

3.3. *Open banking*

The third pillar consists of the imposition of open banking by the second Payment Services Directive (PSD II[58]).

3.3.1. *Open banking as policy approach*

Open banking is the EU's regulatory response to the anti-competitive tendencies of the data economy where the size of the data pool determines competitive strength[59] and where technology firms like Apple, Amazon, Google and others have foregone profits for years to build dominant platforms.[60] At the core are network effects, including across economies of scope and scale, leading to the potential for industry concentration and even dominance. At the extreme, data-driven industries are even potentially subject to "winner takes all" outcomes, with the potential for significant benefits followed by significant negative externalities.

As the leading example, U.S. tech and data markets have tended towards oligopoly or monopoly over time,[61] a process which seems to have occurred in China as well[62] – both of them being jurisdictions which have allowed commercial enterprises to acquire control of large consumer and other data pools. The core assets of those platforms are the

---

Privacy Regulation does come into force, it might impact on financial intermediaries in the future.

[58]Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 Nov. 2015 on payment services in the internal market, O.J. 2015, L 337/35.

[59]See Vezzoso, "Fintech, access to data, and the role of competition policy" in Scortecci and Bagnoli (Eds.), *Competition and Innovation* (2018), available at <ssrn.com/abstract=3106594> (last visited 6 Nov. 2019).

[60]See generally Zachariadis and Ozcan, *The API economy and digital transformation in financial services: The case of open banking,* SWIFT Institute Working Paper 2016-001, 15 June 2017, available at <ssrn.com/abstract=2975199>; see on the PSD II's approach Valcke, Vandezande and Van de Velde, *The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4,* SWIFT Institute Working Paper 2015-001, 23 Sept. 2015, available at <ssrn.com/abstract=2665973>; Zunzunegui, *Digitalisation of payment services*, Ibero-American Institute for Law and Finance Working Paper 5/2018, 27 Sept. 2018, available at <ssrn.com/abstract=3256281>; Colangelo and Borgogno, *Data, innovation and transatlantic competition in finance: The case of the access to account rule,* EU Law Working Paper 35, Stanford-Vienna Transatlantic Technology Law Forum, 2018, available at <ssrn.com/abstract=3251584> (all websites last visited 6 Nov. 2019).

[61]See Wu, *The Master Switch: The Rise and Fall of Information Empires* (Vintage, 2011) (arguing that American information industries tend to press towards monopolies). See also, on the promise and perils of technology-driven competition, Ezrachi and Stucke, *Virtual Competition: The Promise and Perils of The Algorithm-Driven Economy* (Harvard University Press, 2006).

[62]See Abacus News, The China Internet Report 2018, Oct. 2018, available at <abacusnews.com/china-internet-report/china-internet-2018.pdf> (last visited 6 Nov. 2019).

data pools with access to ever-broadening forms of data from users, participants and others. Once this data pool is assembled, it can be used for targeting advertising, undercutting prices, offering new tailored services faster to more clients, or data analysis in all markets where superior information benefits profits.

Competition/antitrust scholars argue that where investors reward growth over profit, predatory pricing becomes highly rational and striving for dominance, even where this is costly, is a worthwhile strategy since it ensures monopoly rents due to control over the essential infrastructure on which their rivals depend.[63] This has prompted the policy demand to treat data as a product, since information and data although different from traditional goods and services, pose problems familiar to competition/antitrust law, such as monopolistic behaviour and collusion.[64] Treating data as a product becomes a particular consideration in avoiding potential reductions in innovation and therefore in long-term growth and development.[65]

By giving providers access to customers' financial information, PSD II opens the way for new banking products and services and facilitates the change of customers from one bank or service provider to another, and thus seeks to reduce the incentives for the predatory pricing identified above. With the EU functioning as first mover, other jurisdictions are considering whether and how to follow.[66] This renders the EU PSD II experiment particularly valuable and significant, not only in payments but also from the standpoint of the real impact of open banking and competition especially from non-traditional technology-focused competitors, including FinTechs and TechFins (data or tech companies moving into financial services, such as Amazon and Alibaba/Ant Financial).[67]

3.3.2. *PSD II's impact on financial services*

---

[63]See Khan, "Amazon's antitrust paradox", 126 *Yale Law Journal* (2017), at 710 (arguing that: "This dual role also enables a platform to exploit information collected on companies using its services to undermine them as competitors."); Rahman and Khan, "Restoring competition in the U.S. economy" in Abernathy, Konczal and Milani (Eds.), *Untamed: How to Check Corporate, Financial and Monopoly Power* (2016), at 18 (arguing that the potential harms from dominance of platform firms include lower income and wages for employees, lower rates of new business creation, lower rates of local ownership, and outsized political and economic control in the hands of a few); see also ACCC, Digital Platforms Inquiry: Preliminary Report, Dec. 2018, available at <accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf> (last visited 6 Nov. 2019).

[64]See Patterson, *Antitrust Law in the New Economy: Google, Yelp, LIBOR, and the Control of Information* (Harvard University Press, 2017) (arguing in favour of conceptualizing information and user and use data as a product, since information and data although different from traditional goods and services, poses problems familiar to antitrust law, such as monopoly and collusion).

[65]These debates are increasingly a major feature not only of the EU but also in the context of the US, other countries around the world, and even China. See "Mark Zuckerberg says he wants more regulation for Facebook", *The Economist*, 6 Apr. 2019.

[66]See Review into Open Banking in Australia: Final Report (Dec 2017), available at <treasury.gov.au/consultation/c2018-t247313/> (last visited 6 Nov. 2019); Leonard, "Regulatory trends and emerging practices in access to customer data, portability and data sharing in the financial services sector", *Data Synergies Pty Limited*, 3 Dec. 2017, available at <ssrn.com/abstract=3154275> (last visited 6 Nov. 2019).

[67]Zetzsche, Buckley, Arner, and Barberis, op. cit. *supra* note 4, at 393.

PSD I[68] and its amending and complementary legislation adopted from 2007 through 2012[69] established the common European market in payment services with the Single Euro Payments Area (SEPA) framework. PSD I led to significant cost reductions in the payments sector through harmonization of the EU Single Market for payment transactions. PSD II was designed to take payments regulation a step further, with a view to significant technical innovation, in particular the "rapid growth in the number of electronic and mobile payments and the emergence of new types of payment services in the market place, which challenges the current framework".[70] PSD II is based on the premises that "significant areas of the payments market, in particular card, internet and mobile payments, remain fragmented along national borders" and that the existing framework suffered from "legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas".[71]

As is often the case, the EU legislation seeks to "square the circle": in addition to addressing the security risks relating to electronic payments[72] as well as extraterritorial payment transactions,[73] PSD II seeks to enable:

> "new means of payment to reach a broader market, [while] ensuring a high level of consumer protection in the use of those payment services across the [EU]. This should generate efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonized payments market".[74]

In response to tech innovation, PSD II introduces two new categories of internet payment services: payment initiation services (PIP)[75] and account information services (ISP).[76] PIPs and ISPs establish "a software bridge between the website of the merchant and the online banking platform of the payer's account"[77] that can be used for payment initiation on the basis of a credit transfer. It is the additional use of information that provides the

---

[68]See Directive 2007/64/EC of the European Parliament and of the Council of 13 Nov. 2007 on payment services in the internal market, O.J. 2007, L 319/1.
[69]See Regulation (EC) 924/2009 of the European Parliament and of the Council of 16 Sept. 2009 on cross-border payments in the Community and repealing Regulation (EC) 2560/2001, O.J. 2009, L 266/11; Directive 2009/110/EC of the European Parliament and of the Council of 16 Sept. 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, O.J. 2009, L 267/7; Regulation (EU) 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro, O.J. 2012, L 94/22; Directive 2011/83/EU of the European Parliament and of the Council of 25 Oct. 2011 on consumer rights, O.J. 2011, L 304/64.
[70]PSD II, Recital 3.
[71]Ibid., Recital 4.
[72]Ibid., Recital 7.
[73]Ibid., Recital 8.
[74]Ibid., Recital 6.
[75]Ibid., Art. 4(15): "payment initiation service" means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.
[76]Ibid., Art. 4(16): "account information service" means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.
[77]Ibid., Recital 27.

benefits to clients. In turn, PIPs and ISPs usually do not at any stage of the payment chain hold the user's funds.[78] Both PIPs and ISPs require direct or indirect access to the payer's account, or the account data, respectively. In order to provide its services, and even to demonstrate its benefits to clients, and similar to the GDPR's consent rule discussed above (at 3.2.1.), the service provider must ask each client for consent to first have access to the data and then to use the data.[79]

PSD II rests on two ways to achieve new clients' consent. First, the service provider could find out who the clients are and seek their consent directly. The service providers however are assumed to be new entrants, and therefore not to know who the clients of a particular payment institution are, so they cannot seek consent in the absence of support by the payment institutions. Given that client contact is the payment institutions' core asset, they have little incentive to let new providers contact their clients.

Second, the service provider may tap into the existing data pool and contact the clients for consent directly if the payment institution is unwilling to support the provider. Under PSD I, bank confidentiality requirements prevented providers from doing so. In order to unlock the potential for innovation in payment services, and based on the recommendations provided by the Open Banking Working Group (OBWG)[80], PSD II requires that banks share customer data relating to payment services with technology firms even where the payment institutions have not entered into a contract with the respective (new) service provider.[81]

PSD II thus plays a central role in pushing forward the transition to data-driven finance in Europe's Single Payments Market and potentially more broadly.

On the one hand, it allows technology firms to enter the payment markets. In light of incumbents' control over client data, and due to the limitation that payment institutions must share client data only with certain additional (tech-driven) service providers, only where a new entrant meets that definition can it hope to gain access to client data. This alone inspires innovative firms to focus on development of value-added services, accelerating the development of data-driven finance in Europe.

On the other hand, payment institutions must respond to PSD II by providing data interfaces (APIs: application programming interfaces) for third party providers from which those providers can extract data of existing clients of the incumbents to provide value-added services. This will increase competitive pressures: banks' only rational response to defend what is increasingly becoming their most valuable asset as the evolution of data-driven finance moves forward – client data – will be to enhance service levels and so avoid their clients seeking those value-added services elsewhere. The costs for these additional value-added services will need to be kept as low as possible. The only way to do so will be to rely more heavily on technology, through advanced analytical tools and models which form the core of the evolution towards data-driven finance.

By mandating the transfer of customer data to third parties – in many cases their new FinTech, and TechFin, as well as traditional, competitors – when directed to do so

---

[78]Ibid., Recital 31.
[79]Ibid., Art. 64.
[80]See EBA Open Banking Working Group, *B2B Data Sharing: Digital Consent Management as a Driver for Data Opportunities* (2018), available at <abe-eba.eu/media/azure/production/1979/eba_2018_obwg_b2b_data_sharing.pdf> (last visited 6 Nov. 2019).
[81]See Arts. 66 and 67 PSD II.

by their customers, such data will have been collected and digitized, repackaged for delivery to regulators and/or internal use and managed by new purpose-built systems, typically all at great expense and difficulty. PSD II thereby sets the stage for the next level of the evolution of data-driven finance: broad competition among incumbent and new participants.

While unintended, another outcome is nonetheless clear. A precondition for the smooth functioning of PSD II is a system for making identification of customers easier, to enable them to more readily access financial services while at the same enhancing financial integrity through better customer identification and tracking, the subject of the following section.

3.4. *Digital identification and ownership transparency*

The fourth element of the transition to data-driven finance is digital identification. The development of digital identification in the EU rests on three building blocks. First is the eIDAS Regulation and its various implementing acts.[82] Second is a new form of corporate identification, the Legal Entity Identifier (LEI), an often overlooked part of MiFID II (and an increasing number of other legislative acts[83]). Finally, corporate and individual systems are being brought together through new requirements for (beneficial) ownership transparency of entities combined with new and stricter anti-money laundering (AML) and customer due diligence requirements introduced by AMLD IV and V.

3.4.1 *eIDAS passport for digital ID*

The eIDAS Regulation provides mutually recognized digital identity for cross-border electronic interactions between European citizens, companies and government institutions. Member states can notify the European Commission of their national form of eID, from September 2018. When an eID is recognized throughout the EU, an individual is able to use it in any Member State,[84] with the eID being assigned a certain level of assurance based on its security specifications.[85] This allows national forms of digital identity to be recognized throughout the EU, and enables any EU citizen or entity so identified to enter into transactions digitally anywhere in the EU.

The goal has been to create a European internal market for e-trust services by ensuring that eIDs work across borders, and have the same legal status as traditional paper-based processes.[86] Use cases include submitting tax declarations,[87] enrolling in a foreign university, remotely opening a bank account, setting up a business in another

---

[82]See Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, O.J. 2014, L 257/73.

[83]For an overview of all financial intermediaries and exchanges mandated to report the LEI see ESMA, *Briefing: Legal Entity Identifier* (LEI), ESMA 70-145-238 (9 Oct. 2017).

[84]See Bastin, Hedea and Cisse, Deloitte*, A Big Step toward the European Digital Single Market*, (Oct. 2016), at 70–77, available at <deloitte.com/lu/en/pages/about-deloitte/articles/inside/inside-issue13.html> (last visited 6 Nov. 2019).

[85]Ibid.

[86]See European Commission, <bit.ly/2p9FH5P> (last visited 6 Nov. 2019).

[87]Thereby, eIDASR is potentially linked to the EU implementation of the G20/OECD Common Reporting Standard (CRS for tax information sharing).

Member State, and bidding for tenders.

The eIDASR is a useful model for eID projects outside the EU since it provides, in principle, an open standard not limited to EU jurisdictions. Every national ID system that wants to connect to the eIDAS system can do so. Connecting to the eIDASR does not require reform of national eID standards. Rather, by defining nodes (so-called eIDAS connectors) that provide the cross-border links between other countries' systems and one's own system, any country could link to the eIDAS identification system in the EU/EEA, resulting – potentially – in a global eID network.

The eIDASR lays the foundation for a service-oriented ID base and for the establishment of electronic know-your-customer (eKYC) utilities in Europe. As the European Commission's Consumer Financial Services Action Plan[88] has pointed out, the "Commission will facilitate the cross-border use of electronic identification and know-your-customer portability based on eIDAS to enable banks to identify customers digitally".[89]

3.4.2. *Digital identification of entities through LEIs*

The introduction of the Legal Entity Identifier (LEI) extends a strategy developed and implemented for OTC derivatives regulation by the G20 and the Financial Stability Board in the aftermath of the 2008 Crisis[90] to all financial market entities dealing with EU counterparties. The LEI is a 20-character, alpha numeric code uniquely identifying a given legal entity. LEI registration requires information about corporate ownership/control. LEIs are overseen globally by the Legal Entity Identifier Regulatory Oversight Committee (LEI ROC), operationalized through the Global LEI Foundation (GLEIF).[91] Any LEI can be tracked and allocated to its owner on the GLEIF website.[92]

LEI reporting requirements were first set in the EU in EMIR, requiring use of LEIs in the context of OTC derivatives transactions and reflecting the internationally agreed approach.[93] Provisions mandating the compulsory use of LEIs with significant degree of

---

[88]See Commission, Consumer Financial Services Action Plan: Better Products, More Choice (March 2017), available at <ec.europa.eu/info/publications/consumer-financial-services-action-plan_en> (last visited 6 Nov. 2019). The Action Plan draws on previous work, such as a commissioned study asking for connection eIDAS and the consumer financial services sector, see CEPS/UCC/LIST, Study on the role of digitalization and innovation in creating a true single market for retail financial services and insurance (1 July 2016), available at <ec.europa.eu/info/publications/study-impact-digitalisation-eu-single-market-consumer-financial-services_en> (last visited 6 Nov. 2019).

[89]See CEPS/UCC/LIST, Study on the role of digitalization and innovation in creating a true single market for retail financial services and insurance (1 July 2016), available at <ec.europa.eu/info/publications/study-impact-digitalisation-eu-single-market-consumer-financial-services_en> (last visited 6 Nov. 2019).

[90]Cf. FSB, FSB Report Global Legal Entity Identifier for Financial Markets (June 2012), available at <fsb.org/2012/06/fsb-report-global-legal-entity-identifier-for-financial-markets/> (last visited 6 Nov. 2019).

[91]See <gleif.org> (last visited 1 July 2019).

[92]See <gleif.org/en/lei-data/access-and-use-lei-data> (last visited 1 July 2019).

[93]See Art. 9 EMIR.

detail[94] are now to be found across and throughout EU financial regulation.[95]

These requirements have allowed the digital identification of legal entities involved in financial transactions in the EU and enabling datafication of a wide range of financial transactions including details of the counterparties. Any legal entity is now identified by a unique number: a digital identity. This digital identity then allows the linkage of many different forms of data to support application of data analytics processes underpinning efficiency and commercial operations, risk management, regulatory processes and new business development.

3.4.3. *Transparency of ownership interests: AMLD IV and V*

EU anti-money laundering (AML) legislation – driven *inter alia* by concerns about tax avoidance (particularly following the Panama Papers revelations) and related G20 agreements around transparency of beneficial ownership – brings all the various legal and regulatory elements in data-driven finance together. While the fourth AMLD (2015)[96] required registration of all significant beneficial ownership interests in business entities, the fifth AMLD (2018)[97] grants the general public access to beneficial ownership data of EU-based companies, requires all financial intermediaries to consult the beneficial ownership register when performing AML due diligence, and creates central access mechanisms to bank account and safe deposit box holder information throughout the EU, thereby ending the anonymity of European accounts.

Linking all data of potential customers that are natural persons through eIDAS and business organization data of legal entities through access to the business organization registers stipulated by the 4th and 5th AMLD with LEIs and related data and reporting requirements, is a game changer for data-driven finance: a significant part of any financial institution's back office is ensuring client identity and suitability of products for clients. A first step of the potential of datafying these activities is provided by the British proposal that besides opening the register for all user groups (which is mandated by AMLD V), seeks to ensure data correctness by cross-checking these data with other databases run by public institutions.[98] Through linking digital identification and

---

[94]See Arts. 26 and 27 of MiFIR and the Commission Delegated Regulation (EU) 2017/590 of 28 July 2016 supplementing Regulation (EU) 600/2014 with regard to regulatory technical standards for the reporting of transactions to competent authorities, O.J. 2017, L 87.

[95]See all financial legislation implementing LEI reporting requirements on <www.leiroc.org/lei/uses.htm> (last visited 6 Nov. 2019). Examples includes the CRR (for credit and financial institutions), AIFMD (funds and fund managers), the Credit Rating Agencies Regulation (CRAR: credit rating agencies and rated entities), Solvency II (pension funds and insurance companies), the Central Securities Depository Regulation (CSDR: CSDs and CSD participants), the Transparency Directive (issuers of EU listed financial instruments), the Securities Financing Transactions Regulation (SFTR: parties to securities financings), and the Prospectus Regulation (public issuers).

[96]See Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, O.J. 2015, L 141/73.

[97]See Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, O.J. 2018, L 156/43.

[98]See UK Department for Business, Energy & Industrial Strategy, Corporate Transparency and Register Reform - Consultation for legislation on options to enhance the role of Companies House and increase the transparency of UK corporate entities, 9 May 2019, pp. 53 et seq.

AML/CDD data with golden source government data sources for purposes of verification and completeness, this proposal promises substantial reductions in customer on-boarding costs and substantial increases in the integrity of on-boarding processes. This could well lead the financial system to the tipping point where data-driven finance is more trustworthy than human-based relationship banking, or at the least considerably more efficient that existing processes of AML/CDD and customer on-boarding.

4. Towards a single data-driven financial market

4.1. *Combined effects*

Summarizing the previous sections, it is clear that individually and in combination, the four separate EU initiatives discussed (digitization of financial regulatory reporting, comprehensive data protection and governance regime, mandatory open banking, and digital ID/ownership transparency) independently drive forward the digitization and the datafication of finance in the EU Single Market, for both market participants and regulators. Cumulatively, they also are driving the next stage of evolution of the European financial sector: the rise of data-driven finance. Financial intermediaries and supervisory authorities could respond to any of these initiatives, on a stand-alone basis, with modifications of existing IT infrastructure. It is the combined effect of the four initiatives that requires a total rethinking of a firm's business proposition. To give one example, intermediaries could focus on data interfaces to meet the digital reporting requirements, but interface programming does not suffice to meet the remaining policy demands. Further, if the GDPR mandates data governance, while PSD II may mandate the data transfer to competitors, and at the same time clients must be identified under the digital identification initiatives and reported under the digital reporting rules, firms need to think twice which data of their clients' preferences they store (of course, with the clients' consent), given that their competition may benefit from it.

While the process is still evolving, the final outcomes are likely to see incumbent financial market participants, innovative FinTechs, big TechFins and other providers (particularly BigTech and telecoms) increasingly competing with one another using ever-broader data sets, with competition being around the analytics as data becomes increasingly portable. While customer relationships were the incumbent's core asset in the past, the ability to analyse large volumes of data appears increasingly to be now replacing them.

In addition to their impact within the EU, each of these discrete sets of regulatory reforms is also effective extraterritorially in many ways, for firms and others engaging in financial services with EU customers or dealing with EU customer data. Thus, data-driven finance as a result of the combination of initiatives in the EU is requiring global attention, and often related strategies and significant expenditures in compliance and implementation of necessary IT and other systems can be seen.

As discussed in section 3 above, financial intermediaries have often collected large amounts of data from and about their customers, over long periods of time. However, in many cases, this data was not used effectively, because it was restricted to certain business units, lines, products or silos within individual firms. The process of

digitization combined with the systemization to meet the requirements of GDPR has triggered a revolution in financial industry treatment of customer data, in the same way that MiFID II and its financial regulatory relatives have driven a revolution in financial industry collection and processing of business and regulatory data.

However, unlike the financial regulatory reforms which underpin digitization and datafication through the application of analytics to massive amounts of data – providing the impetus for data-driven finance in Europe's traditional financial industry – GDPR creates barriers to centralization of individual customer data and their use, placing requirements on the financial industry to develop new systems of data management and also shifting control of many aspects of their data from financial and data intermediaries (which have collected it) to individual customers (who are the subject of it).

The interaction between data and financial regulation has already emerged as one of the most significant issues facing finance and its regulation over the coming years. Finance has long been an information industry,[99] but financial regulation and data regulation evolved in distinctive non-interactive legal silos, based on very different underlying principles and policy objectives. How the financial sector and regulators come to terms with the interaction of these sets of rules will determine in many ways the future of data-driven finance in Europe and around the world.

Limitations on pooling and restrictions on cross-border storage and use of data are also encouraging significant research and spending on new systems of data aggregation and analysis which do not require individual data access, but rather are based on query-only or decentralized structures. These are driving innovation in data systems and analytics. Thus, while regulation places limits on data-driven finance, it also drives it forward in new ways through its focus on the use, collection, storage, transfer and protection of data.

The transformative role of FinTech around the world highlights how finance, data and technology are now all tethered one to the other.[100] As such, regulatory approaches in each area will interact with approaches taken in other areas. The EU provides a vivid example of this through the interaction of key legislation which came into effect in 2018: MiFID II, GDPR, PSD II and eIDAS/AMLD V. It is this combination of regulatory approaches and policies which are pushing forward, and will continue to push forward, data-driven finance in the EU.

The policy concerns that have driven the development of the four EU pillars discussed here are incentivizing an increasing range of other jurisdictions around the world to consider how best to approach the intersection of data, finance and regulation. For these jurisdictions, the experience of the EU provides major lessons for policy and regulatory choices of how to balance financial regulation, data protection, and cybersecurity with competition/antitrust policy and regulation.[101]

---

[99]We initially described finance as a data industry, but upon reflection this is not so – finance is only now slowly evolving into a data industry. Historically, information resided in parts of a bank and was not even shared efficiently across the institution, let alone analysed and applied effectively.

[100]See generally EBA, Report on the Prudential Risks and Opportunities Arising From FinTech (3 July 2018); EBA, Report on the impact of fintech on the incumbent credit institutions' business model (6 July 2018).

[101]The topic of competition/antitrust policy, however, is beyond the scope of this paper.

4.2. *Data regulation as financial regulation*

As mentioned, existing regulation will need to be reshaped to better accommodate the demands - and potential - of the rise of data-driven finance, particularly through interactions with data protection regulation. Budgets for IT, cybersecurity, and IT risk will all need to grow substantially and even more rapidly than in the past, not only in the private sector but also, and particularly, in regulatory and supervisory bodies.

In addition, however, there is a more fundamental question regarding regulatory approaches to data-driven finance beyond those embodied in RegTech: in particular the interaction between data regulation and financial regulation. To date, the impact of *laissez-faire* approaches to regulation of private sector use of data can be seen in the US and China, both of which are now characterized by the dominance of their data sectors by small numbers of participants.[102] In both cases, this has arguably been facilitated by few limits on individuals transferring ownership and control of data to BigTech firms, which in turn have benefited from network effects and economies of scope and scale in its amalgamation and use.

This has repercussions for the objectives of financial law and regulation and hence the remits of regulators and supervisors: Where the power is in the data, we would recommend that financial regulators focus on the new systemic and other risks stemming from concentration of data in the hands of a few technology firms, as a complement to traditional approaches to systemic risk represented by banks that were too-big-too-fail or too-connected-too-fail. In turn, we support market structure-related interventions which aim to maintain the independence of, and choice among, critical infrastructure providers as well as data portability rights in favour of financial customers, in order to comply with overarching objectives such as financial stability, financial innovation, development and inclusion, financial integrity, and consumer protection.

4.3. *Challenges for data-driven finance*

Not all that glitters is gold. Not all the EU's experiences are positive. The EU's road to digital finance comes with a number of unforeseen roadblocks providing challenges policy makers need to address in the years to come. Four caveats in particular are of relevance.

First, implementing reforms is costly for traditional financial intermediaries. Customers may experience the multi-layer financial and data regulation as burdensome. In addition, the significant penalties for data protection violations come on top of penalties for violating financial law. All of this impacts on the profitability of licensed intermediaries. In turn, the number of registered credit institutions is shrinking, and so potentially does competitive pressure in the European market. It is yet to be seen whether the regulatory changes will in fact spur the hoped-for new entrants and competition.

Second, scale economies associated with data tend to press for size. While the EU has required the financial industry to develop appropriate systems for data management and limited the use the industry can make of pooled data (thereby reducing the advantages

[102]See Cavanillas, Curry, and Wahlster in Cavanillas, Curry and Wahlster (Eds.), *New Horizons for a Data-Driven Economy* (Springer, 2016).

of traditional financial institutions through their data pools), it has also driven the standardization of data processes outside finance – potentially contributing a larger data pool and enabling new entrants to access more data of their individual customers. In other words, data is now more freely transferable than before.

For instance, the results of PSD II could be different from what is expected. PSD II's objective is to enhance competition. Due to the data portability rights under PSD II, the door is open for large technology firms that know best how to use these data portability rights (which are not identical to the data portability rights under GDPR that are designed to favour consumers) to enter financial services markets. These large technology firms are much better equipped to do so than new entrants for which access to customers is limited by budgets and resources. While aiming at increased competition, the outcome may well be the concentration of data-driven services in the hands of a few technology firms that provide financial services as one aspect of their data-driven business models.

Third, data-driven supervision is a different skill from more traditional form-based approaches. Accordingly, while the judgement calls may be similar, the information will be far more granular and up-to-date, and a different skill set may well be necessary for data-driven business oriented financial supervision. Overall, we expect more statistical, in a way more "academic", approaches to supervision where decisions are taken based on empirically based probability assumptions rather than case-by-case scrutiny of files.

Fourth, data-driven finance requires fewer human resources for customer contact and account management, and more bank staff with technological, risk assessment and trouble shooting skills. This will mean fewer less skilled, lower paid jobs, and more highly skilled, better paid jobs. This will be good for some potential employees, but not for many existing ones.

5. Driving digital finance

In this article, we have argued that a series of seemingly uncoordinated projects is playing a crucial role in reshaping Europe's financial ecosystem to make it more open to innovation by data-driven financial services providers (of an increasing range of forms) than ever before. Overall, Europe's path to data-driven finance is the result of the interaction of four separate legal frameworks developed and implemented for separate reasons but coming together to cause a digital transformation of European finance. In doing so, the EU is providing a globally significant case study for regulators and policy makers from around the world. However, what the EU did without an overarching roadmap, other jurisdictions may – and we argue should – impose purposefully, through careful development of coordinated legal and regulatory approaches to finance, data and their interaction.

In the EU, the framework for data-driven finance is a robust rule of law environment (that ensures the viability of long-term investments), a strict approach to data privacy that grants data portability rights to individuals rather than service providers, a willingness to use regulation to drive evolution of markets and societies, and an approach aiming at "controlled" rather than "cutthroat" capitalism.

In this respect, the EU approach was enabled by a "traditional" cultural bias

against data commercialization. This political and social environment was further supported by the European Commission and the European regulatory authorities (particularly ESMA and the European Banking Authority) playing a strong central role in developing regulatory frameworks to address key policy challenges around data and finance. Without the emergence of various new central EU regulators in the field of finance that could extend their activities without long-standing bureaucratic legacy issues, few steps towards data-driven finance would have been possible in financial supervision.

The EU's experience with its separately designed policy and regulatory frameworks considered here will have a very important determinative impact on the structure of data-driven finance, not only in the Single Financial Market, but also in global financial markets, particularly as other jurisdictions consider how best to balance the objectives of data protection and financial regulation while supporting innovation, efficiency and financial stability, and many of them look for role models. This will be driven by the familiarity of many institutions with the EU framework as a result of having to implement its requirements for their European operations and even globally as a result of its extraterritorial reach. The change from extending finance on the basis of what an institution knows directly about its customers to extending it on the basis of data analytics drawing upon huge pools of data is profound, with the potential for both highly positive as well as highly negative outcomes as this evolution plays out across not only Europe, but the world.

In looking at these issues, based on experiences to date, we would suggest a number of central lessons. The first is that finance, data and technology are now intertwined as a result of a long-term process of digitization and datafication of finance. Consequently, the use of technology for compliance, monitoring, enforcement, and system design in financial regulation – RegTech – of necessity will continue to increase.[103]

The second lesson is that each society must grapple with its own approach to data and its role in its future. The discussions will have to involve not only questions of finance and data regulation, but also of social regulation and competition regulation. These issues must be addressed, because otherwise globalization and network efforts will likely mean that decisions taken elsewhere will dictate the outcomes in other markets around the world. While there appears to be a strong divergence of attitudes towards the use of data by governments around the world, there appears to be an increasing consensus around placing limits on the use of data by the private sector.

The third is that because of the integration of data and finance, when designing financial regulatory systems and seeking to regulate data, it is necessary to consider – during the design process – the implications of the interaction of data and finance. As can be seen from the EU experience, conflicts between objectives and rules should be considered *ex ante*. One area where this is particularly important is in choices about whether to pursue open banking and digital ID strategies. At this point the EU experience is at a very early stage, but it will be determinative of the approach taken in many other jurisdictions: success or failure will echo around the world.

---

[103]For a detailed analysis of the RegTech dimension, see Buckley, Arner, Zetzsche and Weber, "The Road to RegTech: The (astonishing) example of the European Union", 20 *Journal of Banking Regulation* (2019).

Looking forward, we suggest that most jurisdictions will need both a general data regulation framework – where societal differences are likely to result in very different approaches and outcomes as well as possible fragmentation – and one that operates specifically in the context of finance, where societal differences are likely to be much less important and where financial regulatory objectives around transparency and information sharing are likely to dominate. Likewise, it will be central to consider how best to balance the positive roles of data and finance, with their potential for negative and potentially even dystopian outcomes.