Faculty of Law,
Economics
and Finance

Law Working Paper Series
Paper number 2019-005

The Future of Data-Driven Finance and RegTech

Lessons from EU Big Bang II

Dirk A. Zetzsche, University of Luxembourg
Dirk.Zetzsche@uni.lu

Douglas W. Arner, University of Hongkong
douglas.arner@hku.hk

Ross P. Buckley, University of New South Wales
ross.buckley@unsw.edu.au

Rolf H. Weber, University of Zurich
rolf.weber@rwi.uzh.ch

01/03/2019

UNIVERSITÉ DU LUXEMBOURG

EBI Working Paper Series

2019 – no. 35

Dirk A. Zetzsche/Douglas W. Arner/

Ross P. Buckley/Rolf H. Weber

The Future of Data-Driven Finance and RegTech:

Lessons from EU Big Bang II

26/03/2019

The European Banking Institute

The European Banking Institute based in Frankfurt is an international centre for banking studies resulting from the joint venture of Europe's preeminent academic institutions which have decided to share and coordinate their commitments and structure their research activities in order to provide the highest quality legal, economic and accounting studies in the field of banking regulation, banking supervision and banking resolution in Europe. The European Banking Institute is structured to promote the dialogue between scholars, regulators, supervisors, industry representatives and advisors in relation to issues concerning the regulation and supervision of financial institutions and financial markets from a legal, economic and any other related viewpoint. The Academic Members of EBI are the following:

1. Universiteit van Amsterdam, Amsterdam, The Netherlands
2. Universiteit Antwerpen, Antwerp, Belgium
3. Πανεπιστήμιο Πειραιώς / University of Piraeus, Athens, Greece
4. Alma Mater Studiorum – Università di Bologna, Bologna, Italy
5. Academia de Studii Economice din București (ASE), Bucharest, Romania
6. Universität Bonn, Bonn, Germany
7. Trinity College, Dublin, Ireland
8. Goethe-Universität, Frankfurt, Germany
9. Universiteit Gent, Ghent, Belgium
10. Helsingin yliopisto (University of Helsinki, Helsinki, Finland)
11. Universiteit Leiden, Leiden, The Netherlands
12. Universidade Católica Portuguesa, Lisbon, Portugal
13. Universidade de Lisboa, Lisbon, Portugal
14. Univerze v Ljubljani / University of Ljubljana, Ljubljana, Slovenia
15. Queen Mary University of London, London, United Kingdom
16. Université du Luxembourg, Luxembourg
17. Universidad Autónoma Madrid, Madrid, Spain
18. Universidad Complutense de Madrid/CUNEF, Madrid, Spain
19. Johannes Gutenberg University Mainz (JGU), Mainz, Germany
20. University of Malta, Malta
21. Università Cattolica del Sacro Cuore, Milan, Italy
22. Πανεπιστήμιο Κύπρου / University of Cyprus, Nicosia, Cyprus
23. Radboud Universiteit, Nijmegen, The Netherlands
24. Université Panthéon - Sorbonne (Paris 1), Paris, France
25. Université Panthéon-Assas (Paris 2), Paris, France
26. Stockholms Universitet/University of Stockholm, Stockholm, Sweden
27. Tartu Ülikool / University of Tartu, Tartu, Estonia

EBI Working Paper Series

EBI Working Paper Series are a project of the European Banking Institute e.V.. EBI Working Paper Series represent a selection of academic researches into the area of banking regulation, banking supervision and banking in general which have been drafted by professors and researchers of EBI Academic Members and selected by the Editorial Board.

Editorial Board

THE FUTURE OF DATA-DRIVEN FINANCE AND REGTECH: LESSONS FROM EU BIG BANG II

DIRK A. ZETZSCHE DOUGLAS W. ARNER

ROSS P. BUCKLEY AND ROLF H. WEBER

[2019] *UNSWLRS* 22

UNSW Law
UNSW Sydney NSW 2052 Australia

THE FUTURE OF DATA-DRIVEN FINANCE AND REGTECH: LESSONS FROM EU BIG BANG II

Dirk A. Zetzsche[*]
Douglas W. Arner[†]
Ross P. Buckley[‡]
Rolf H. Weber[§]

March 2019

ABSTRACT

Europe's path to digitization and datafication in finance has rested upon four apparently unrelated pillars: (1) extensive reporting requirements imposed after the Global Financial Crisis to control systemic risk and change financial sector behavior; (2) strict data protection rules reflecting European cultural concerns about dominant actors in the data processing field; (3) the facilitation of open banking to enhance competition in banking and particularly payments; and (4) a legislative framework for digital identification imposed to further the European Single Market.

The paper analyzes these four pillars and suggests that together they will underpin the future of digital financial services in Europe, and – together – will drive a Big Bang transition to data-driven finance. These seemingly unrelated pillars together bolster an emerging ecosystem which aims to promote a balance among a range of sometimes conflicting

* 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 Co-Founder, 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" and the Hong Kong Research Grants Council Research Impact Fund as well as participants at the European Banking Institute annual conference in Frankfurt in February 2019 for their comments and Pamela Cela, Tsany Ratna Dewi, Zak Vidor Staub and Robin Veidt for their most helpful research assistance.

objectives, including systemic risk, data security and privacy, efficiency, and customer protection. Furthermore, we argue Europe's financial services and data protection regulatory reforms have unintentionally driven the use of regulatory technologies (RegTech) by intermediaries, supervisors and regulators, thereby laying the foundations for the digital transformation of both EU financial services and financial regulation. The experiences of Europe in this process provide 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 Data Protection Regulation (GDPR), Open Banking, Payment Services Directive 2 (PSD 2), RegTech.

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

Contents

INTRODUCTION

Extensive regulatory reforms imposed as the result of the Global Financial Crisis (GFC) have caused dramatic structural changes in finance around the world. The GFC 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 also been a major driving factor in the adoption and use of new technologies in the sector, particularly the technologies that aid compliance with regulation, known as RegTech.[2] In parallel with, and increasingly coupled to, these financial regulatory reforms, have occurred extensive reforms of data protection, the advent of open banking, and the development of digital identification regimes. Together, these four factors are forming a regulatory ecosystem that supports a transformative transition from traditional banking and finance to data-driven banking and finance. This paper explores how these four areas of regulatory reforms, each introduced for their own discrete reasons, are interacting today in Europe to drive the development and adoption of RegTech solutions, and, more fundamentally, are supporting the transition to data-driven financial services – a transition which we characterize as a new "Big Bang" of data driven finance and RegTech.

One of the greatest challenges facing the financial industry globally today is the at times conflicting requirements of data regulation and financial regulation. Yet, as demonstrated by the latest U.S. Federal Trade Commission's (FTC) policy initiative that requires financial institutions to protect the privacy and security of the customers' data,[3] among the greatest questions from the standpoint of societies are those around the nature of

---

1 *See*, e.g., ROSS P. BUCKLEY, EMILIOS AVGOULEAS & DOUGLAS W. ARNER (EDS), RECONCEPTUALIZING GLOBAL FINANCE AND ITS REGULATION (2016); ROSS P. BUCKLEY & DOUGLAS W. ARNER, FROM CRISIS TO CRISIS: THE GLOBAL FINANCIAL SYSTEM AND REGULATORY FAILURE (2011).

2 Douglas W. Arner, Janos Barberis & Ross P. Buckley, *FinTech, RegTech and the Reconceptualisation of Financial Regulation*, 37 NW. J. INTERN. L. & BUS. 371-414 (2017); Institute of International Finance, *RegTech in Financial Services: Technology Solutions for Compliance and Reporting* (March 2016); Douglas W. Arner, Janos Barberis, & Ross P. Buckley, *The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data*, 44 J. FIN. TRANSFORMATION 79 (2016); Luca Enriques, *Financial Supervisors and Regtech: Four Roles and Four Challenges*, REVUE TRIMESTRIELLE DE DROIT FINANCIER 53 (2017).

3 See The Federal Trade Commission (FTC), Press Release, 'FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules', March 9, 2019, *available at*: https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules (proposing to introduce broad new requirements for financial institutions to protect the privacy and security of the customer information by amending a pair of rules promulgated under the Gramm-Leach Bliley Act).

finance and the digital economy, as well as the role of data, technology and regulation in societies going forward. As this paper demonstrates, there is much to learn from a detailed analysis of the EU's experience with implementing one of the world's first systems for regulating both finance and data, one that governs finance and data in the EU itself and also extends extraterritorially to all those interacting with EU markets and citizens from around the world. Beyond questions of the interaction between financial and data regulation are questions around the role of technology in regulation, compliance and digital financial transformation, i.e. the role of RegTech both in supporting the process of transition and providing the basis of a system to address its requirements, monitor compliance and support the achievement of regulatory and policy objectives by regulators and policymakers. There has been little analysis, so far, as to how a comprehensive RegTech system for data-driven finance could and should be developed in a given financial system. This paper seeks to explore the relationship between financial regulation, data protection and RegTech and the evolution of finance in the EU. Drawing on the European case and experience, we argue that these four factors together are providing a regulatory ecosystem that supports the transformative transition from relationship-based to data-driven banking and finance.

In Part I, we evaluate FinTech, RegTech and data-driven finance. In Part II, we analyze the four EU regulatory frameworks which, with the benefit of hindsight, have empowered the growth of RegTech solutions and kickstarted the EU into a major transformation towards an economy based on data-driven finance. RegTech in Europe developed rapidly with the introduction of extensive, purely digital, reporting from intermediaries to regulators, pursuant to new financial legislation imposed after the Global Financial Crisis including, inter alia, the Alternative Investment Fund Managers Directive (AIFMD 2011[4]) and the European Markets Infrastructure Regulation (EMIR 2012[5]), the fourth Capital Requirements Directive and the Capital Requirements Regulation (CRD IV[6]/ CRR[7]) in

[4] *See* Directive, 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, OJ L 174, 1.7.2011, p. 1–73.

[5] *See* Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, OJ L 201, 27.7.2012, p. 1–59.

[6] *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, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, OJ L 176, 27.6.2013, p. 338–436.

[7] *See* Regulation (EU) No 575/2013 of the European Parliament and of the Council

2013, and the reformed Markets in Financial Instruments Directives (MiFID II[8]) in 2014 (Part II.1.). This was followed by the rigorous data protection demanded by the General Data Protection Regulation (GDPR[9]) (Part II.2.), which has fundamentally altered how all firms – including financial services firms – deal with personal data. The third measure was the imposition of open banking by the second Payment Services Directive (PSD 2[10]) requiring that incumbent intermediaries must share client data with new competitors (Part II.3.). The fourth facilitative measure was cross-border digital identity pursuant to the eIDAS framework[11] that establishes a network of national identity providers which can be either public or private (Part II.4.).

Overall, Europe's road to data-driven finance and RegTech is the result of the interaction of these four separate legal frameworks implemented for separate reasons but coming together to provide an environment which is transforming European finance and has both demanded, and supported, a RegTech revolution. In doing so, Europe is providing a globally significant case study for regulators and policy makers from around the world on questions relating to regulation of data-driven finance and the use of RegTech.

In Part III we compare these EU developments with other major jurisdictions, in particular the United States, China and India. Europe differs from the US mainly with regard to its unique, privacy-oriented approach to data protection, reinforced by its approach to data portability and open banking. The main difference of Europe from China lies in data protection and data privacy, with respect to the roles of the state and private sector. Both the US and China have taken a different approach to data regulation than Europe. This has allowed the emergence of a small group of BigTech /

---

of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, OG L 176, 27.6.2013., p. 1-337.

[8] *See* Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJ L 173, 12.6.2014, p. 349–496.

[9] *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, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, at 1–88.

[10] 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 of 23.12.2015, L 337/35.

[11] *See* Regulation (EU) No 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, OJ L 257, 28.8.2014, at 73–114.

TechFin[12] firms in the US and China in an environment of low regulation, in contrast to the densely regulated environment of Europe. Europe's main difference from India is the lack of a centralized strategy to underpin digital financial transformation, with Europe characterized by a less coordinated approach across major areas. While these markets are at very differing stages of development, they are all nonetheless characterized by being large jurisdictions, with rapidly evolving environments for finance and data. Going forward, these are the markets others will consider when determining their own approaches to questions of financial regulation, data regulation, and RegTech.

In Part IV we put the European developments into context, consider the lessons learned from other jurisdictions and formulate policy recommendations. In particular, we 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.

Part V concludes.

I. FINTECH, REGTECH AND THE ORIGINS OF DIGITAL FINANCE

Financial technology (FinTech) is growing rapidly and creating new opportunities through big data,[13] the Internet of Things (IoT),[14] artificial intelligence (AI) / machine learning,[15] distributed ledger technology and

[12] Dirk A. Zetzsche, Ross P., Douglas W. Arner & Janos N. Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 14 NYU J. L. & BUS. 393 (2018).

[13] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L.R. 1904 (2013); Solon Barocas, Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CA. L. REV. 671 (2016); Daniel M. 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 L. J. 909 (2013); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECHN. & INTELLECTUAL PROPERTY 239 (2013); Dirk A. Zetzsche, Ross P., Douglas W. Arner & Janos N. Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 14 NYU J. L. & BUS. 393 (2018).

[14] 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 ROLF H. WEBER/ROMANA WEBER, INTERNET OF THINGS: LEGAL PERSPECTIVES, (Zurich, 2009).

[15] 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* DAVID

blockchain,[16] smart contracts,[17] and digital identity,[18] among others. Sometimes this occurs through regulatory arbitrage or regulatory avoidance; sometimes it is the direct result of the implementation of regulation. Crowdfunding,[19] digital currencies,[20] initial coin offerings,[21] touchless and e-payment solutions[22] and robo advisors[23] all display the breadth of FinTech applications evolving to avoid regulation. In many cases, though, these

---

POOLE, ALAN MACKWORTH & RANDY GOEBEL, COMPUTATIONAL INTELLIGENCE: A LOGICAL APPROACH, at 1 (1998); STUART J. RUSSEL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH (3rd ed. 2009). Russel and Norvig prefer the term "rational agent".

[16] *See* C. Catalini & J.S. Gans, *Some Simple Economics of the Blockchain*, Rotman School of Management Working Paper No. 2874598 (September 21, 2017); MIT Sloan Research Paper No. 5191-16, *available at* https://ssrn.com/abstract=2874598; Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 4 U. ILL. L. REV..1361-1406 (2018); Usah Rodrigues, *Law and the Blockchain*, 104 Iowa L. Rev. 679 (2019).

[17] Jeremy M. Sklaroff, *Smart Contracts and* the *Cost of Inflexibility*, 166 U. Pa. L. Rev. 263 (2017); K Werbach & N Cornell, *Contracts Ex Machina*, 67 Duke L. J. 313 (2017); M Raskin, *The Law and Legality of Smart Contracts*, 1 GEORGETOWN L TECHN. REV. 304 (2017); Lin W. Cong & Zhiguo He, *Blockchain Disruption and Smart Contracts*, Working Paper (May 22, 2018), *available at* https://ssrn.com/abstract=2985764; Rolf H. Weber, *Smart Contracts: Do We Need New Legal Rules?* In DIGITAL REVOLUTION – NEW CHALLENGES FOR LAW (De Franceschi/Schulze/Graziadei/Riente/Sica/Sirena, eds., forthcoming 2019).

[18] Douglas W. Arner, Dirk A. Zetzsche, Ross P. Buckley & Janos Barberis, *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, 20 EUR. BUS. ORG. L. REV. 55-80 (2019), *available at* https://ssrn.com/abstract_id=3224115.

[19] *See* Georg Gutfleisch, *Crowdfunding and Initial Coin Offerings Under The EU Legal Framework*, 15 EUR. COMPANY L. J. 73 (2018); Dirk Zetzsche & Christina Preiner, *Cross-Border Crowdfunding Towards a Single Crowdfunding Market*, 19 EUR. BUS. ORG. L. REV. 217 (2018).

[20] *See* Hossein Nabilou & Andre Prüm, *Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies*, 5 J. FIN. REG. 1 (2019).

[21] Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, 60 HARVARD INT'L L. J. (forthcoming 2019), *available at* https://ssrn.com/abstract=3072298; Shaanan Cohney, David A. Hoffman, Keremy Sklaroff & David A. Wishnick, *Coin-operated Capitalism*, COLUMB. L. REV. (forthcoming 2019); Marco dell'Erba, *Initial Coin Offerings: The Response of Regulatory Authorities*, 14 NYU J. L. & BUS. 1109 et seq. (2018); Saman Adhami, Giancarlo Giudici & Stefano Martinazzi, *Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings*, J. ECON. & BUS. (forthcoming 2019), *available at* https://ssrn.com/abstract=3046209.

[22] Phillip Maume, *In Unchartered Territory – Banking Supervision Meets Fintech*; CORP. FIN. 272 (2017).

[23] *See* Wolf-Georg Ringe & Christopher Ruof, *A Regulatory Sandbox for Robo Advice*; EBI Working Paper Series 26/2018.

innovations have the potential to reduce transaction costs or the need for intermediaries – the latter in a phenomenon referred to as disintermediation or disruption. At the same time, one of the biggest drivers of technology spending in financial services (and the growth of the compliance industry) is the implementation of financial regulatory requirements, with BCBS239's risk data aggregation requirements being paradigmatic.[24]

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. 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.[25] The clash of cultures of traditional bankers 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 investors and clients of financial intermediaries will be negative. FinTech has not abolished risks. It has altered the type of some existing risks and added new risks, including one we have referred to as Global Technology Risk (GTR).[26]

As laid out in previous research, the new risks created by FinTech can be addressed by new approaches to regulation (which we have termed Smart Regulation[27]) paired with regulatory and supervisory technologies (collectively referred to as RegTech).

'RegTech' is a contraction of 'regulatory' and 'technology',[28] and describes the use of technology, particularly information technology ('IT'), for regulation, monitoring, reporting and compliance.[29] RegTech has

---

[24] Basel Committee on Banking Supervision, *Principles for Effective Risk Data Aggregation and Risk Reporting* (2013).

[25] *See* Douglas W. Arner, Dirk A. Zetzsche & Ross P. Buckley, *FinTech, RegTech and Systemic Risk: The Rise of Global Technology Risk*, in, SYSTEMIC RISK IN THE FINANCIAL SECTOR: TEN YEARS AFTER THE GLOBAL FINANCIAL CRISIS (Douglas W. Arner Emilios Avgouleas, Danny Bush & Steven Schwarcz eds., 2019 forthcoming).

[26] *See id*.

[27] *See* Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner & Janos N. Barberis, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, 23 FORDH. J. CORP. FIN. L. LAW 31-103 (2017); *see also* Rolf H. Weber & Rainer Baisch, *FinTech – Eligible Safeguards to Foster the Regulatory Framework*, 33/10 J.I.B.L.R. 335-350 (2018).

[28] *See* Ernst & Young, *Innovating with RegTech* (2016), *available at* http://www.ey.com/Publication/vwLUAssets/EY-Innovating-with-RegTech/$FILE/EY-Innovating-with-RegTech.pdf.

[29] Arner, Barberis & Buckley, RegTech, *supra* note 2, at 4; Rolf H. Weber, *RegTech as A New Legal Challenge*, 46 J. FIN. TRANSFORMATION 10 (2017).

initially evolved to address regulatory challenges in the financial system through innovative technology. It can support the technical handling of large amounts of data, sophisticated analysis of data and automated data processing within intermediaries as well as between intermediaries and supervisors. Examples of RegTech include electronic Know-Your-Customer (KYC) systems which facilitate client on-boarding by financial intermediaries as well as enhancement of market integrity,[30] 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.

RegTech differs from FinTech in that FinTech mostly addresses business processes, while RegTech concerns the relationship between intermediary and supervisor and/or regulator; i.e. RegTech ensures not only that the law is complied with more effectively, meaning either a higher degree of compliance, or the same degree of compliance at lower cost, but also provides systems for designing better regulatory and supervisory systems and infrastructure. FinTech by definition also involves only the financial sector, whereas RegTech can apply in any area of regulation, compliance and system design, whether in the context of finance or otherwise.[31]

In light of its benefits the common view among regulators and scholars is that RegTech is, in principle, desirable. Nascent research on the functions of RegTech argues that RegTech could include the use of technology for enhancing operations (framed by Luca Enriques as 'Operations RegTech'[32]), for increasing compliance controls ('ComplianceTech'), for intensifying or improving financial supervision ('OversightTech' or 'SupTech'), and for influencing the legislature ('PolicyTech'). RegTech can subsume all of these, in the context of use of technology for regulatory and compliance purposes by industry, regulatory and policymakers. At the same time, there is a consensus that RegTech (like FinTech) brings new challenges, including for supervisors the need for qualified human resources and adaptations in internal governance as well as new cybersecurity risks.

FinTech and RegTech involve both financial regulation and data protection regulation. This intersection of finance and data that lies at the heart of FinTech and RegTech is also central to the emergence of data-driven finance. This raises challenges for regulators in dealing with sometimes conflicting policy objectives and systems. However, it also provides an opportunity for us to think about how regulatory systems can shape the future evolution of data-driven finance and the role of RegTech in

30 Arner, Zetzsche, Buckley, Barberis, Identity, *supra* note 18, at 7.

31 To the broader scope of RegTech *see also* Weber, *supra* note 26, at 11.

32 *See* Enriques, *supra* note 2, at 4.

supporting financial efficiency, integrity and stability going forward, which form the subjects of the second Part of this paper.

II. THE EUROPEAN BIG BANG 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 1980s.[33] These have included the 1986 Single European Act,[34] which established the key formative plan for integration in the context of the single market and which was also one of the triggers for the financial reforms in the UK known as "Big Bang"[35]; the 1992 Maastricht Treaty[36] establishing the EU as well as the structure of the single market and the single currency; the 1995 White Paper on enlargement[37]; European Economic and Monetary Union (EMU) in 1999 combined with the 1999 Financial Services Action Plan[38]; the 2001 Lamfalussy Report[39]; the 2009 de Larosiere Report in the aftermath of the 2008 Global Financial Crisis[40]; and Banking Union in the aftermath of the 2010 Eurozone Crisis.[41]

We suggest in this section that 2018 and the implementation of four separate legislative reforms should be seen as a new Big Bang – a Big Bang II – in the EU: one of data-driven finance and its regulation. We argue that the impact of the 2018 Big Bang II will be transformative to European finance over the coming years and will be as important a milestone as those which have taken place before. However, unlike the list in the preceding

---

[33] For the evolution of the EU Single Financial Market, the role of financial regulation and implications for global finance, *See* Emilios Avgouleas & Douglas W. Arner, *The Eurozone Debt Crisis and the European Banking Union: "Hard Choices", "Intolerable Dilemmas" and the Question of Sovereignty*, 50 THE INTERN'L LAWYER 29, 29-67 (2017); Douglas W. Arner & Ross P. Buckley, *Redesigning the Architecture of the Global Financial System*, 11 MELBOURNE J. INTERN'L L. 185, 185-239 (2010); Rolf Weber & Douglas W. Arner, *Toward a New Design for International Financial Regulation*, 29 U. PA. J. INTERN.'L L. 391, 391-453 (2007).

[34] OJ L 169, 29.6.1987.

[35] *See* Jamie Robertson, BBC News, *How The Big Bang Changed the City of London for ever*, (27 Oct. 2016), *available at* https://www.bbc.com/news/business-37751599.

[36] Treaty on European Union, Feb. 7, 1992.

[37] Preparation of the Associated Countries of Central and Eastern Europe for Integration into the Internal Market of the Union - White Paper. COM(95) 163 final, May 3, 1995.

[38] EUROPEAN COMMISSION, Financial SERVICES ACTION PLAN (1999).

[39] EUROPEAN COMMISSION, THE FINAL REPORT OF THE COMMITTEE OF WISE MEN ON THE REGULATION OF EUROPEAN SECURITIES MARKETS, Feb. 15, 2001.

[40] THE HIGH-LEVEL GROUP ON FINANCIAL SUPERVISION IN THE EU, Report, Feb. 25, 2009.

[41] *See* Avgouleas & Arner, *supra* note 33.

paragraph, Big Bang II has not been a carefully designed strategy to support further integration and evolution of finance in the EU.

Rather, the four legislative measures analyzed in this part were all implemented for separate reasons, but their combined effect has been to give an extraordinary, unanticipated impetus to the digital transformation of finance and RegTech in the EU. The measures are the digital regulatory reporting requirements particularly of AIFMD and MiFID II, the rigorous data protection of GDPR, the open banking regime introduced by PSD 2 (particularly combined with the data portability requirements in GDPR), and the pan-European digital identity framework built pursuant to eIDAS. Each is considered in turn.

A. Extensive, Digital Regulatory Reporting Obligations: From AIFMD to CRR and MIFID II

Since the 2008 Crisis, in tandem with post-crisis international regulatory approaches, European regulators have imposed ever higher reporting obligations on financial intermediaries in an effort to combat systemic risk as well as address a range of integrity risks emerging from money laundering, terrorism financing and competition scandals (in particular those around LIBOR and foreign exchange trading). The most important regulatory initiatives in this regard include, for the banking sector CRR/CRD IV (finalized in 2013 and effective in 2014), for the asset management sector the AIFMD (2011 / 2013), for financial markets MiFID II/MiFIR (2014 / 2018), for market infrastructure the EMIR (2012 / 2013), for payment services PSD 2 (2015 / 2018), and for money laundering the AMLD 5 (Anti-Money Laundering Directive 2018 / 2020).

These frameworks share a common focus related to international financial regulatory standards in the EU; and a common imposition of extensive reporting requirements upon the financial services industry. Regulators in the EU, by requiring financial intermediaries to report far more data on their decisions, activities and exposures, have triggered a RegTech revolution in Europe's regulated financial industry. It is a given today that when faced with a proposed regulation, 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 are collected within their organization to meet reporting requirements, that these data are packaged and reported in the necessary structure and form, and that they flow from the supervised

entities to the supervisors in the required manner.

This has also forced regulators and supervisors to develop data management systems which are capable of receiving and processing the volume of data being generated and delivered by the financial services industry. This process of digitization of reporting and related compliance requirements across both intermediaries and regulators has led to a RegTech "revolution" in the European financial services industry.

In addition, as the industry has digitized and standardized data has been collected across the global operations of individual firms, it has also begun to focus on better using the data being collected, both to reduce compliance costs and generate new opportunities. This is the process of datafication: the application of analytics tools to digital data, i.e. the fundamental process of digital financial transformation and the evolution of data-driven finance in the traditional financial services industry.

In addition, as supervisors have been deluged with ever-increasing volumes of data, in digitized standard forms, supervisors have also had to enhance their data analytics tools. Once their analytics tools are enhanced, supervisors can handle even more data (and in turn, tend to ask the supervised entities to collect and transmit even more of it, triggering another RegTech cycle).

As an example, when fund managers were required by the AIFMD in 2011 to report extensive data on investment strategies in a purely digital manner,[42] there was an outcry from small and mid-size firms arguing they would be disadvantaged relative to the large fund managers. Time has solved this problem. Seven years later the data stream from fund managers via national competent authorities (NCAs) to ESMA (the European Securities and Markets Authority) flows smoothly. We expect the same with regard to other regulatory initiatives if sufficient implementation time is granted; the latest example being the MiFID II implementation with its extensive reporting requirements and extraterritorial impact.

Perhaps the clearest example comes from a UK FCA enforcement action against Merrill Lynch in October 2017, in which the firm was fined just over GBP 34.5m for failing to report some 68.5 million exchange traded derivatives transactions between 12 February 2014 and 6 February 2016,[43] as required under EMIR and MiFID.[44] From the standpoint of data-driven finance, the case highlights how the financial industry has been fully

---

[42] *See* Dirk A. Zetzsche & David Eckner, *Investor Information and Reporting*, in THE ALTERNATIVE INVESTMENT FUND DIRECTIVE (Zetzsche, ed., 2018).

[43] *See* FCA, *FCA Fines Merrill Lynch £34.5 Million for Failing to Report Transactions*, *available at* https://www.fca.org.uk/news/press-releases/fca-fines-merrill-lynch-failing-report-transactions

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

digitized and datafied: for how else could 68.5 million exchange traded transactions even occur over a two-year period, amounting to more than two transactions per second? At the same time, it also highlights the role of EU financial regulatory requirements in driving RegTech in financial services: for only through the use of technology could Merrill Lynch ever report the transactions at the frequency required. The market conduct that gave rise to this enforcement action therefore emphasizes the role of data-driven finance. It also highlights the role of RegTech for otherwise the chances of the FCA knowing of the failure would be low, as it could not first accept the necessary digital reports and then subject them to appropriate analytics.

In passing, the action also highlights the utter inadequacy of many penalties imposed on banks by regulators: GBP 34.5 m represents a 50 pence penalty for each derivative transaction Merrill Lynch failed to report, surely one of the few bargains on offer in London today.

Early results of the data streams to ESMA can now be seen: for instance, ESMA has published comparative reports on fund fees[45] and a catalogue of financial instruments traded at European stock exchanges.[46]

This development, examined elsewhere,[47] is central to the process of Europe's digital financial transformation because this regulatory evolution has forced the financial services industry (and its regulators) to digitize data collection and regulatory reporting comprehensively.

The next element of the process of digital transformation and the evolution of RegTech in Europe arises from the regulatory framework addressing the data and their collection, use, storage and protection.

B. Data Protection: GDPR

The EU *General Data Protection Regulation* (*GDPR*) is the most important change in data regulation since the first Data Protection Directive of 1995,[48] not only in the EU but to a large extent globally. It has been – due to its exterritorial effect as stated in the Recitals and in Article 3(2)

---

[45] *See* ESMA, *The Impact of Charges on Mutual Fund Returns* in REPORT ON TRENDS, RISKS AND VULNERABILITIES, No. 2 (2017).

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

[47] *See* Veerle Colaert, *RegTech as a Response to Regulatory Expansion in the Financial Sector*, Working Paper (June 2018), *available at* https://ssrn.com/abstract=2677116; Rodrigo Zepeda, *The 2018 Big Bang*, Working Paper (Aug. 2017), *available at* https://ssrn.com/abstract=3029145.

[48] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

GDPR[49] – a game changer for data collection and processing in the EU and worldwide.[50]

EU financial regulatory reporting requirements have driven digitization and datafication of finance and its regulation, causing a massive increase in RegTech and the transition to data-driven finance in Europe's traditional financial services industry. GDPR – while impacting all sectors of the economy – has triggered a similar process in the collection, use, storage and protection of data in the financial sector. As financial regulation drove the digitization of data, GDPR has driven spending on systems designed to appropriately manage that ever-increasing volume of data. Such spending is supporting digitization and datafication not only in the regulated financial industry but also across the entire economy. It is in light of its role as a key driver of data-driven finance and RegTech that we next consider GDPR.

1. Basic Principles of GDPR

In the EU, Article 8(1) of the European Convention on Human Rights ('ECHR'), Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union ('TFEU') together provide as fundamental rights and freedoms that everyone has the right to the protection of their personal data. An extensive regulatory framework has developed around this over time, with GDPR being the most important

[49] *See* Recital 24, 25 GDPR : '(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes. (25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.' *See also* Article 3(2) GDPR: 'This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.'

[50] The interpretation of the notion of extraterritorial effect has been recently clarified by the European Data Protection Board: EUROPEAN DATA PROTECTION BOARD (EDPB), GUIDELINES 3/2018 ON THE TERRITORIAL SCOPE OF THE GDPR (2018) (Article 3) – Version for public consultation, adopted on 16 November 2018.

evolution of this framework. Specifically, GDPR imposes rules that seek to protect natural persons in relation to the processing of their personal data.[51]

According to the GDPR:

> '[r]apid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.'[52]

GDPR is thus a response to the substantial increase in cross-border flows of personal data between public and private actors, including natural persons, associations and undertakings across the EU[53]:

> '[n]atural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and [is expected to] further facilitate the free flow of personal data within the [EU] and the transfer to [non-EU countries] and international organisations.'[54]

In addition, EU law calls upon national authorities in the EU Member States to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another EU Member State,[55] which is also a key focus of GDPR.

In this environment, and based on the premise that the creation of trust is a crucial precondition for further developing the digital economy across the European internal market,[56] GDPR seeks to ensure a high level of protection of personal data, through a 'strong and more coherent data protection framework in the [EU], backed by strong enforcement.'

GDPR is designed to be technology neutral, i.e. it does not depend on the techniques used for data collection and processing in order to prevent circumvention[57] :

---

51 *See* Recital 1 GDPR.
52 *See* Recital 6 GDPR.
53 *See* Recital 5 GDPR.
54 *See* Recital 6 GDPR.
55 *See* Recital 5 GDPR.
56 *See* Recital 7 GDPR.
57 *See* Recital 15 GDPR.

> ‘The protection of natural persons should apply to [any] processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system.’[58]

GDPR is restricted to data processing of personal data in connection with a professional or commercial activity (in contrast to an individual’s household activity). However, the controllers or processers of social media or other providers of software for household activities are subject to the GDPR.[59]

2. Consent and Ownership

The most important building block of the GDPR is that natural persons should have control of their own personal data. This right does not apply to legal persons, however, given that legal persons do not benefit from the fundamental rights granted by the ECHR, the Charter and the TFEU. The key GDPR tool for control is the consent requirement stipulated by Article 6 (1) (a) GDPR.[60] Natural persons must be clearly informed of the data collected as well as the purposes for which the personal data are used. 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.

---

58 *See* Recital 15 GDPR.

59 *See* Recital 18 GDPR.

60 *See* on the consent requirement Recital 40 GDPR: ‘[I]n order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.’ *See also* Recital 42 GDPR:

> ‘Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.’

Even where consent has been given, the circumstances under which consent has been achieved will be reviewed to remedy coercive pressure to achieve consent:

> 'In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.'[61]

GDPR further provides considerable detail on how consent must be achieved:

> 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or 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. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.'[62]

In addition, the data collected cannot be stored forever, but must be deleted in timeframes that relate to the objective for which the data was collected. Following the Google Spain decision of the Court of Justice,[63] the

---

61 *See* Recital 42 GDPR.

62 *See* Recital 32 GDPR.

63 *See* Case C-131/12, Google Spain SL and google Inc. v Agencia Esanola de

GDPR further establishes a right to be forgotten upon request of the natural person (understood as withdrawal of consent), where the data have been unlawfully processed or where the personal data are no longer necessary for the purposes for which they were collected or processed.[64] This in many ways is targeting both the potentially undesirable impact of network effects and economies of scope and scale in data and their possible tendency toward undesirable natural monopolies.

The ownership 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 without hindrance from the current controller. The right to data portability is driven by antitrust law considerations but is applicable irrespective of the existence of a data controller's dominant market position. This approach is reinforced further specifically for the banking industry in the context of PSD 2's open banking provisions. However, in fact, GDPR likewise imposes portability across the entire economy, not only in the context of payments, a subject we return to subsequently.

3. Data Management and Compliance Requirements

In addition to the mentioned fundamental principles, importantly in EU data protection law, the GDPR contains a number of specific data organization requirements. It furthers the use of pseudonymisation of personal data as a measure to 'reduce the risks to the data subjects and help controllers and processors to meet their data-protection obligations.'[65] It also regulates the use of online identifiers[66] and imposes rules on tracing and profiling of

---

Proteccion de Datos (AEPD) and Mario Coteja Gonzales, 2014 E.C.R 317; *see also* Rolf H. Weber, *On the Search for an Adequate Scope of the Right to Be Forgotten*, 6 JIPITEC 2 (2015).

64 *See* Article 17 (1) GDPR.

65 *See* Recital 28 GDPR. *See also* Recital 29 GDPR:
'In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.'

66 *See* Recital 29 GDPR:
'Natural persons may be associated with online identifiers provided by their

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.[67]

Article 25 GDPR also introduces the requirements of "privacy by design" and "privacy by default". These principles were originally developed and promoted by the Canadian Ontario Data Protection Commissioner, Ann Cavoukian.[68] Article 25(1) GDPR reads as follows:

> 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical measures, such as pseudonomization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of the data subjects.'

Consequently, the enterprises are obliged to implement privacy-friendly technologies into their technical systems.

Furthermore, in case of using new technologies causing substantive privacy risks, controllers of data are bound by the obligation to undertake data protection impact assessments; the details of which are described in Article 35 GDPR. In addition, the security of data processing has become a key issue of the GDPR. According to Article 31, controllers and processors are obliged to implement specific data security (technical and organizational) measures that should help to identify and mitigate the respective risks.

Cross-border data transfer has been a hotly debated issue for many

---

devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.'

[67] *See* Article 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.

[68] *See* Ann Cavoukian & Alex Stoianov, *Biometric Encryption*, 15(3) Biometric Technology Today 11 (2007).

years. In respect of private enterprises, the GDPR has now introduced a set of rules for transfers of personal data to third countries or international organizations – such transfers are legitimate 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 44-47 of GDPR.

In addition, there are also new rules for the public sector: The GDPR addresses significant issues for regulators, particularly in the context of cross-border sharing of information – a core element of both pre- and post-2008 international regulatory initiatives. Technically, GDPR does not extend to public authorities such as those involved in public security and crime prevention,[69] tax and customs authorities, financial investigation units, or financial market authorities.[70] These public authorities are subject to more specific legal requirements the EU has adopted for crime prevention.[71] If such specific sectorial legislation does not exist, general data protection requirements tailor-made for public institutions apply.[72] However GDPR is nonetheless significantly impacting the practices of financial regulators and their interactions with the financial industry – which is subject to the requirements of GDPR – resulting in potential questions about the legality of submitting information to regulators about the activities of individual customers, such as in the context of AML or other financial regulatory reporting requirements. These arise in particular with the interactions between EU financial institutions and data about EU natural persons and the possible transfer to non-EU regulators (such as those in the US).

The detailed provisions of the GDPR are paired with severe 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

---

69 *See* Recital 19 GDPR.

70 *See* Recital 31 GDPR.

71 *See* 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 prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA.

72 *See* Article 60 GDPR and Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L8, 12.1.2001, at 1. In addition, EU law provides for many specific provision of data processing by public authorities in sectorial legislation. For instance, *See* with regard to financial legislation, the respective provisions in the CRD IV, the MiFID II, the AIFMD, the PSD2 and others.

handling her personal data, even in the absence of contractual relationships between the person and controller/processor.[73] At the same time, GDPR comes with heavy penalties, up to 4% of the total worldwide annual turnover of the corporate group to which the data controller or processor belongs.[74]

The early months of GDPR practice have left little doubt that the European data protection authorities are willing to impose sizable penalties.[75]

4. Driving the Next Stage of Data-Driven Finance and RegTech

In the context of European finance, GDPR's initial impact comes from its requiring financial intermediaries to reorganize their data processing as well as client data policies to meet the requirements of GDPR. The extensive details on personal data of individuals also require data categorization tools which allow for amendments and deletion after a given timeframe or upon the natural person's request.

Financial intermediaries have often collected large amounts of data from and about their customers, over long periods of time. However, in many cases, these data have not been used effectively, because they have been restricted to certain business units, lines, products or silos within individual firms.[76] Financial intermediaries are now obliged to build comprehensive systems for their digitized data which address the collection, storage, use and protection of the data according to the principles of the 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.

However, unlike the financial regulatory reforms which drive not only

---

[73] *See* Article 82 (1) GDPR.

[74] *See* Article 83 GDPR.

[75] *See* Charlie Osborne, *Facebook Could Face $1.63bn Fine Under GDPR Over Latest Data Breach*, ZERO DAY (Oct. 2, 2018) https://www.zdnet.com/article/facebook-could-face-billions-in-fines-under-gdpr-over-latest-data-breach/: the first high fine was imposed by the French Data Protection Authority in January 2019, amounting to 50 million Euro 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 1.63bn for its Cambridge Analytica scandal.

[76] *See* Luiz Awazu Pereira da Silva & Goetz von Peter, Bank for International Settlements, *Financial Instability: Can Big Data Help Connect the Dots?*,(2018), *available at* https://www.bis.org/speeches/sp181203.pdf.

digitization but also datafication through the application of analytics to massive amounts of data – providing the impetus for data driven finance in Europe's traditional financial industry as well as the rapid evolution of RegTech – GDPR instead 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.[77] Furthermore, data pools relating to the past become increasingly 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, in other words, RegTech.

By establishing data processing rules the GDPR has interfered in the internal organization of data intensive businesses, such as social media, health or financial institutions.

However, 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 of traditional financial institutions through their data pools), it has also driven the standardization of data processes outside of finance – potentially making for a larger data pool and enabling new entrants to potentially access more data of their individual customers. In other words, data are now more freely transferable than before. Large technology companies know well how to

[77] The EU has introduced a specific data protection regime governing electronic communications, namely Directive 2002/58, *see* EUR-Lex https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058. This Directive will be replaced shortly at the time of writing by a so-called E-Privacy Regulation, *see* European Commision, Proposal for an ePrivacy Regulation (2018), *available at* https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation, coordinated with and simultaneously with the implementation of the GDPR. However, political objections, particularly in respect of the proposed cookies rules, have caused a major delay and it is not year clear when this Directive will come into force; nevertheless, it might influence the financial intermediaries in the future.

make use of the new rights to data transfer – and much better so than new entrants with access to customers limited by budgets and resources. This could prompt unexpected results: while originally designed to curtail the power of data behemoths the result of GDPR may be less competition from the greater concentration of data in the hands of the few.

C. Open Banking: PSD 2

As if this were not enough however the Second Payments Services Directive (PSD 2)[78] mandates that banks now will have to transfer customer data to third parties – in many cases their new FinTech, and TechFin, as well as traditional, competitors – when directed to do so by their customers, reinforcing the requirements of GDPR. 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 2 thereby sets the stage for the next level of the evolution of data driven finance: broad competition among incumbent and new participants.

Besides extensive and purely digital reporting to regulators (further reinforcing the RegTech cycle discussed in II.A. above), PSD 2 imposes to a certain degree 'open banking'[79] requirements, whereby incumbent financial intermediaries must share client data with third parties, including potentially innovative new competitors. By giving providers access to the

---

[78] 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; Regulation (EU) No 1093/2010; Repealing Directive 2007/64/EC, OJ of 23.12.2015, L 337/35.

[79] *See generally* on open banking Markos Zachariadis & Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking* SWIFT Institute Working Paper No. 2016-001 (June 15, 2017), *available at*., https://ssrn.com/abstract=2975199; *see* on the PSD 2's approach to open banking, Peggy Valcke, Niels Vandezande & Nathan Van de Velde, *The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4*, SWIFT Institute Working Paper No. 2015-001 (September 23, 2015), *available at*, https://ssrn.com/abstract=2665973; Fernando Zunzunegui, *Digitalisation of Payment Services*, Ibero-American Institute for Law and Finance Working Paper No. 5/2018 (September 27, 2018), *available at* https://ssrn.com/abstract=3256281; Giuseppe Colangelo & Oscar Borgogno, *Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule*, EU Law Working Papers No. 35, Stanford-Vienna Transatlantic Technology Law Forum (2018), *available at* https://ssrn.com/abstract=3251584; Benjamin Geva, *Payment Transactions Under the EU Second Payment Services Directive (PSD2) – An Outsider's View*, 54 TEX. INT. L. J. (Forthcoming 2018), *available at* https://ssrn.com/abstract=3292313 .

clients' financial information, PSD 2 opens the way for new banking products and services and facilitates the change of customers from one bank or service provider to another. With the EU functioning as first mover, other jurisdictions are considering whether and how to follow.[80] This renders the EU PSD 2 experiment particularly valuable and significant not only in payments and RegTech 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.

1. The Advent of 'Open Banking'

Open banking is the regulatory response to the anti-competitive tendencies of the data economy where the size of the data pool determines competitive strength[81] and where technology firms like Amazon, Google and others have foregone profits for years to build dominant platforms. 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, American tech and data markets have tended towards oligopoly or monopoly over time,[82] a process which seems to have occurred in China as well – both jurisdictions which have allowed commercial enterprises to acquire control of large consumer and other data pools. The core assets of those platforms is the data pool with access to both shoppers' and merchants' data. 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.

---

[80] *See* on the Australian Open Banking initiative, *Review into Open Banking in Australia: Final Report* (Dec 2017), *available at* https://treasury.gov.au/consultation/c2018-t247313/; Leonard, Peter G, *Regulatory Trends and Emerging Practices in Access to Customer Data, Portability and Data Sharing in the Financial Services Sector*, Data Synergies Pty Limited (December 3, 2017), *available at* https://ssrn.com/abstract=3154275.

[81] *See* Simonetta Vezzoso, *Fintech, Access to Data, and the Role of Competition Policy*, *in* COMPETITION AND INNOVATION (Scortecci, Bagnoli, Ed., 2018), *available at* https://ssrn.com/abstract=3106594.

[82] *See* TIM 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, ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2006).

Legal 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: 'This dual role also enables a platform to exploit information collected on companies using its services to undermine them as competitors.'[83] 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 behavior and collusion.[84] Treating data as a product becomes a particular consideration in avoiding potential reductions in innovation and therefore in long-term growth and development.

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.

Open banking applies these insights to the payment service sector where the controller of client data controls access to the client, and thus can impede or further access of clients to new services.

2. PSD 2 and Open Banking

PSD 1[85] and its amending and complementary legislation adopted from 2007 through 2012[86] established the common European market in payment

[83] *See* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017); K. Sabeel Rahman & Lina Khan, *Restoring Competition in the U.S. Economy*, in UNTAMED: HOW TO CHECK CORPORATE, FINANCIAL, AND MONOPOLY POWER 18, 18 (Nell Abernathy, Mike Konczal & Kathy Milani, eds., 2016) (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 (December 2018), *available at* https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf

[84] *See* Mark R. Patterson, *Antitrust Law in the New Economy: Google, Yelp, LIBOR, and the Control of Information* (2017) (arguing in favor 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).

[85] *See* 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, at 1.

[86] *See* Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 on cross-border payments in the Community and repealing

services with the Single Euro Payments Area (SEPA) framework. PSD 1 was a success, in harmonizing payment transactions throughout the EU single market, and in achieving significant market integration and related efficiencies in the commercial and consumer payment sector. When PSD 2 was first discussed, the European payments sector was not in need of reform; quite the opposite, European regulatory confidence had just been bolstered by a very successful reform project.

This provided the background for taking payments regulation one step further, addressing the significant technical innovation since the PSD 1 framework had been adopted, 'with 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.'[87] Starting with a strategic Green Paper by the European Commission, in 2012[88] the reform was 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. It has proven difficult for payment service providers to launch innovative, safe and easy-to-use digital payment services and to provide consumers and retailers with effective, convenient and secure payment methods in the Union. In that context, there is a large positive potential which needs to be more consistently explored.'[89]

This positive potential, in particular, referred to the many use cases of financial technology.

Regulation (EC) No 2560/2001, OJ L266, 9.10.2009, p.11; Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7); Regulation (EU) No 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 and amending Regulation (EC) No 924/2009 (OJ L 94, 30.3.2012, p. 22); Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304, 22.11.2011, p. 64).

87 *See* Recital 3 PSD 2.

88 *See* EUROPEAN COMMISSION, TOWARDS AN INTEGRATED EUROPEAN MARKET FOR CARD, INTERNET AND MOBILE PAYMENTS, 11 January 2012.

89 *See* Recital 4 PSD 2.

As is often the case, the European legislation seeks to 'square the circle': PSD 2 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 harmonised payments market.'[90]

PSD 2 also seeks to address the security risks relating to electronic payments[91] as well as extraterritorial payment transactions.[92]

In order to achieve equivalent rules for equivalent transactions, regardless of the technology used, legal form employed or number of transacting parties involved, and ensure equivalent protection for merchants and consumers,[93] PSD 2 introduces a neutral definition of payment transactions.[94] Relating to that definition, the single license prudential framework for all 'payment institutions', i.e. providers of payment services which are not connected to taking deposits or issuing electronic money, set out in PSD 1 and refined and supplemented in PSD 2, applies.

PSD 2 responds, in particular, to new developments regarding internet payment services, such as payment initiation services[95] and account

---

90 *See* Recital 6 PSD 2.

91 *See* Recital 7 PSD 2.

92 *See* Recital 8 PSD 2:
'[W]here one of the payment service providers is located outside the European Economic Area (EEA) in order to avoid divergent approaches across Member States to the detriment of consumers. Where appropriate, those provisions should be extended to transactions in all official currencies between payment service providers that are located within the EEA.'

93 *See* Recital 10 PSD 2:
'This Directive introduces a neutral definition of acquiring of payment transactions in order to capture not only the traditional acquiring models structured around the use of payment cards, but also different business models, including those where more than one acquirer is involved. This should ensure that merchants receive the same protection, regardless of the payment instrument used, where the activity is the same as the acquiring of card transactions. Technical services provided to payment service providers, such as the mere processing and storage of data or the operation of terminals, should not be considered to constitute acquiring. Moreover, some acquiring models do not provide for an actual transfer of funds by the acquirer to the payee because the parties may agree upon other forms of settlement.'

94 *See* Article 2 PSD 2.

95 *See* Article 4 (15) PSD 2: '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

information services.[96] Both types of services 'play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's account in order to initiate internet payments on the basis of a credit transfer.'[97]

Figure: Service Providers under PSD2

held at another payment service provider.' 'Payment initiation services'

> 'enable the payment initiation service provider to provide comfort to a payee that the payment has been initiated in order to provide an incentive to the payee to release the goods or to deliver the service without undue delay. Such services offer a low-cost solution for both merchants and consumers and provide consumers with a possibility to shop online even if they do not possess payment cards.'

See also Recital 29 PSD 2:

> 'Since payment initiation services are currently not subject to Directive 2007/64/EC, they are not necessarily supervised by a competent authority and are not required to comply with Directive 2007/64/EC. This raises a series of legal issues, such as consumer protection, security and liability as well as competition and data protection issues, in particular regarding protection of the payment service users' data in accordance with Union data protection rules. The new rules should therefore respond to those issues.'

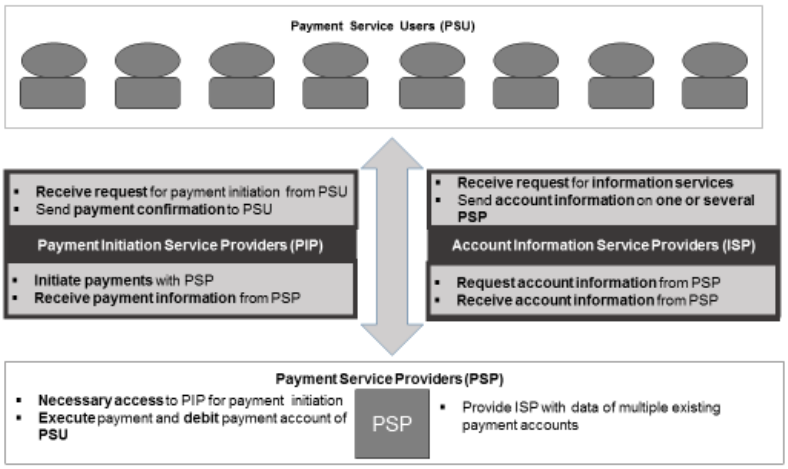
[96] *See* Article 4 (16) PSD 2: 'account information service' means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.' Account information services

> 'provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider. The payment service user is thus able to have an overall view of its financial situation immediately at any given moment.'

See also Recital 28 PSD 2:

> 'Those services should also be covered by this Directive in order to provide consumers with adequate protection for their payment and account data as well as legal certainty about the status of account information service providers.'

[97] *See* Recital 27 PSD 2.



While both kinds of services form crucial parts of the modern payment services chain, both services differ significantly. In particular, '[w]hen exclusively providing payment initiation services, the payment initiation service provider does not at any stage of the payment chain hold the user's funds.'[98] In turn, such a payment initiation services provider will not meet the definition and licensing requirement for payment institutions. However, '[w]hen a payment initiation service provider intends to provide payment services in relation to which it holds user funds, it should obtain full authorization [under PSD 2] for those services.' [99] The same applies to account information services – they rarely hold the funds; it is the additional use of information that provides the benefits to clients. Both payment initiation services and account information services require direct or indirect access to the payer's account, or the account data, respectively. For providing its services, and even demonstrating its benefits to clients, the service provider must ask each client for consent to first have access to the data and then to use the data.[100] This is the result of the GDPR's consent rule laid out above.

There are two ways to contact new clients. First, the service provider could find out who the clients are and seek their consent directly. But the service providers are new entrants, and they rarely 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

98 *See* Recital 31 PSD 2.
99 *See* Recital 31 PSD 2.
100 *See* Article 64 PSD 2.

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 1 bank confidentiality requirements prevented providers from doing so. PSD 2 seeks to unlock the potential for innovation in payment services. Based on the recommendations provided by the Open Banking Working Group (OBWG)[101], PSD 2 requires, in particular, that banks share customer data relating to payment services with technology firms. It does so by granting a right to the user of payment services to make use of payment initiation and account information services, even where the payment institutions have not entered into a contract with the respective (new) service provider.[102] It assigns to clients an ownership right over their data, and provides at the same time a specific use case for the data subject's data portability right granted by Article 20 of GDPR, thereby linking the PSD 2 initiative to the GDPR objective laid out above. This way, PSD 2 aims to create a pro-innovative environment with a high level of customer service, while simultaneously upholding the principles of cybersecurity, data protection *and* financial stability.

3. PSD 2, RegTech and Data-Driven Finance

PSD 2 plays a central role in pushing forward the transition to data-driven finance and in supporting the evolution of RegTech in Europe's Single Financial Market.

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. Naturally, these entities will seek to keep their costs down and respond to regulatory responses like data sharing and liability requirements by technical means, furthering the evolution of RegTech.

On the other hand, payment institutions must respond to PSD 2 by providing data interfaces for third party providers from which those providers can extract data of existing clients of the incumbents to provide

---

101 *See* EBA Open Banking Working Group, *B2B Data Sharing: Digital Consent Management as a Driver for Data Opportunities* (2018), *available at* https://www.abe-eba.eu/media/azure/production/1979/eba_2018_obwg_b2b_data_sharing.pdf.

102 *See* Article 66, 67 PSD 2.

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. This process is then reinforced through the reporting obligations contained in PSD 2 and elsewhere, thereby driving the consequential evolution of RegTech in tandem with data-driven finance.

While unintended, the outcome is nonetheless clear. Taking the process one step forward however is a system for making identification of customers easier, to enable them to more readily access financial services (such innovation and development) while at the same enhancing financial integrity (through better customer identification and tracking), the subject of the following section. All of this enhances financial efficiency and benefits customers. It also makes it easier for new entrants to compete with established financial market participants and for customers to identify and transfer their data to innovative new entrants.

Nonetheless, we do not posit that the results of PSD 2 will be all as expected. PSD 2's objective is to enhance competition. Due to the data portability rights under PSD 2, the door is open for large technology firms that know best how to use these data portability rights (which are thus not identical to the data portability right under GDPR, which is designed to favour consumers) to enter financial services markets. While aiming at increased competition the outcome may well be the opposite: 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.

D. Digital Identity: eIDAS and Beyond

1. Towards Cross-border ID

The eIDAS Regulation was adopted in 2014 to provide 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, and other member states have been able to recognize these voluntarily since 2015, and have

been required to do so since September 2018. When an eID is ultimately recognized throughout the EU, an individual will be able to use it in any member state.[103] The eID is assigned a certain level of assurance based on its security specifications, and this allows states to determine the services in relation to which it may be used.[104]

This system does not make redundant individual sovereign forms of identity. However it does allow national forms of digital identity to be recognized throughout the EU, and thereby enables any EU citizen or entity so identified to enter into transactions digitally.

Rather than introducing a pan-European ID card system, which would have doubled the work for Member States, the eIDASR has sought to ensure people and businesses can use their own national eIDs to access public services in other EU countries where eIDs are available. 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.[105] Use cases include submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another member state, and bidding for tenders.

Prior to eIDASR many different national standards for eIDs, independent from coordinated EU policy, were developed within EU member states. The eIDASR does not harmonize those standards, but focuses on their technical interoperability. By mandating that member states and eID providers meet certain identification obligations (including that the person identification data uniquely represents the person to which it is attributed and that online authentication is available)[106], the eIDASR is designed to create trust in the eIDASR-based cross-border identification.

2. eIDASR as an Open Standard

The eIDASR is a useful model for eID projects 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 own's system any

---

103 *See* R. Bastin, I. Hedea & I. Cisse, Deloitte, *A Big Step toward the European Digital Single Market*, at 70-77 (Oct. 2016), *available at* https://www2.deloitte.com/lu/en/pages/about-deloitte/articles/inside/inside-issue13.html.

104 *Id.*

105 *See* European Commission, http://bit.ly/2p9FH5P.

106 *See* EU No 910/2014, eIDAS regulation, art. 11, 2014.

country could link to the eIDAS identification system in the EU/EEA, resulting – potentially – in a global eID network.

While adopted in 2014, the implementation of the eIDASR took some time, with public eID systems taking the lead. However, in November 2017 the first private sector-run national eID scheme was notified to the European Commission by Italy, connecting all eIDs created by that private enterprise to the European eID network. This enables Italian citizens and businesses to use their Italian eID credentials to access public services in other member states.[107]

3. Towards e-ID-Based RegTech

The eIDASR lays the foundation for a service-oriented ID base and for the establishment of electronic know-your-customer (eKYC) utilities in Europe. The European Commission's Consumer Financial Services Action Plan,[108] aims to 'work with the private sector to explore how they could use electronic identification and trust services for checking the identity of customers.' In particular, Action Item 11 states: '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'.[109] Such eKYC utilities are a major RegTech innovation that promise substantial reductions in customer on-boarding costs for providers, and substantial increases in the integrity of on-boarding processes as nefarious customers are limited in their capacity to shop around for a friendly and compliant, or perhaps inept, financial services provider.

---

[107] *See* European Commission, First private sector eID scheme pre-notified by Italy under eIDAS, 7 December 2017, *available at* http://bit.ly/2DmVQtV, and http://bit.ly/2DmVQtV.

[108] *See* European Commission, *Consumer Financial Services Action Plan: Better Products, More Choice* (March 2017), *available at* https://ec.europa.eu/info/publications/consumer-financial-services-action-plan_en (last access 20 June 2018). 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* https://ec.europa.eu/info/publications/study-impact-digitalisation-eu-single-market-consumer-financial-services_en (accessed on 20 June 2018).

[109] *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* https://ec.europa.eu/info/publications/study-impact-digitalisation-eu-single-market-consumer-financial-services_en (last visited June 20, 2018).

E. Big Bang II

Individually and in combination, it is clear that these four separate EU initiatives – financial regulation, data protection, payments, and digital ID – all independently drive forward the digitization and the datafication of finance in the EU Single Market, from the standpoint of both market participants and regulators. Cumulatively, they also are driving the next stage of evolution of the European financial sector: data-driven finance – a Big Bang II in European finance. While the process is still evolving, based on the legal infrastructure now in place, the final outcomes are likely to see incumbent financial market participants, innovative FinTechs, TechFins and other providers increasingly competing with one another using ever-broader, and more highly analyzed, data sets. While client relationships were the incumbent's core asset in the past, control over large volumes of data now replaces them.

In addition to their impact within the EU, each of these discrete sets of regulatory reforms are also effective extraterritorially in many aspects, for firms and others engaging in financial services with EU customers or dealing with EU customer data. Thus, particularly the impetus for RegTech development as a result of the combination of initiatives in the EU is requiring global consideration, and in many cases development of related strategies and significant expenditures in compliance and implementation of necessary IT and other systems.

It is also clear that the policy concerns that have driven the development of the four EU pillars discussed herein are driving an increasing range of other jurisdictions around the world to consider how best to approach the intersection of data, finance and regulation.

III. EVOLVING APPROACHES TO DATA-DRIVEN FINANCE AND THE ROLE OF REGTECH

The world is currently providing a laboratory of different environments in which data-driven finance and RegTech can operate and evolve.

In the US, a uniquely relaxed approach to privacy and data protection based on a market-based understanding of customer ownership coupled to an overriding distrust of state use of personal data has empowered a huge range of data applications that are increasingly raising concerns, particularly with the emergence of increasingly dominant data players such as Google, Facebook and Amazon.[110]

[110] *See* David McLaughlin, *Why Were Facebook, Amazon, Apple, and Google*

In the EU, we see the converse approach with the GDPR representing so far the global high point of data protection and rigorous information reporting requirements. This has meant the demand for RegTech in the EU is currently outstripping the capacity to generate the IT needed. However, when such systems designed to ensure individual control of data are combined with a distrust of private sector use of consumer data, particularly as is now being seen with US BigTech, a very different possible future emerges.

China has seen a similar pattern of BigTech emerging. In China, BigTech is already increasingly dominating finance.[111] Somewhat ironically given China's history, the private sector, in the form of two of its major internet firms, Tencent and Alibaba, have led the evolution of data amalgamation and use, including by establishing national identification systems to underpin their payments and other systems, and the burgeoning superstructure of RegTech and other financial services applications being built upon them.

India has adopted a comprehensive strategy around digital transformation and the development of data-driven finance through digitization and datafication, termed "India Stack", As the foundational element, Aadhaar is a government-driven, national biometric database and identification system which has empowered financial inclusion and provided the technological foundation for a whole range of RegTech and other innovations.[112] In many ways, India's top-down, state-led approach to designing digital infrastructure is the countermodel to the market driven approaches of the US and China.

We consider these differing approaches and the potential lessons in this section.

A. United States: Free Market and Anti-government

The US has led the world – at least until arguably very recently – in the evolution of data-driven finance as well as in data industries more broadly, on the basis of a combination of the size and competitiveness of US markets

---

Allowed to Get So Big? FORTUNE (2019), *available at* http://fortune.com/2019/03/16/google-amazon-antitrust-laws/.

[111] *See* Caroline Binham, *Big Tech Disrupters May Pose Risk To Financial Stability, Warns Global Regulator*, FINANCIAL TIMES (Feb 15, 2019), *available at* https://www.ft.com/content/f1e67d0e-3085-11e9-8744-e7016697f225.

[112] *See* Unique Identification Authority of India, Government of India, *What is Aadhaar?* (Jan 24, 2019), *available at* https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html.

and pro-market policy choices embedded in the legal and regulatory framework.[113] It has also led the world in the evolution of RegTech. It is thus a major competitor for European finance and was the major example to which others looked prior to 2008.

The US may be characterized historically as having a highly market-oriented approach to both finance and data. The overriding concern has often been to support individual choice. In the US – in contrast to China – policy has generally been driven by a fear of the potential for government overreach and a strong desire to maximize individual freedom of choice.

Until very recently,[114] the result has been an approach to data protection largely driven by freedom of contract, allowing individuals and others to freely transfer ('alienate') data as their property while simultaneously seeking to restrict the use of data by government. The consequence has been the emergence of massive data firms such as Google, Facebook and Amazon.

At the same time, distrust of large financial firms has led to a generally restrictive regulatory environment for financial institutions, albeit one focused mainly on correcting market failures through disclosure.[115] The combination of a disclosure-based financial system, technology innovation, and free alienability of data has underpinned the evolution of RegTech in the US, where technology has been used by financial regulators to enhance their performance at least since the 1980s.

In comparing the US to Europe, since 2008, and disregarding the EU's extensive focus on organizational and operating requirements for intermediaries for reasons of simplicity, financial regulatory approaches to disclosure have been largely similar and focused on enhanced reporting obligations which in turn have driven the use of RegTech in compliance. The use of RegTech in compliance is also beginning to drive RegTech's use by regulators to a new level, building on the fairly high level of digitisation and datafication already present in many US regulators, particularly the SEC, the CFTC, the OCC and FINRA. For instance, the US OCC – contrary to their European counterparts – calculate banks' capital requirements based on operational data reported by the banks.[116] This necessitates very granular

---

113 *See* Louis Lucas & Richard Waters, *China and US Compete to Dominate Big Data*, FINANCIAL TIMES (May 1, 2018), *available at* https://www.ft.com/content/e33a6994-447e-11e8-93cf-67ac3a6482fd.

114 *See* Kiran Stacey, *Senior Democrat Suggests 'Glass-Steagall Law for Tech Companies*, FINANCIAL TIMES (Mar 4, 2019), *available at* https://www.ft.com/content/561b8546-355c-11e9-bd3a-8b2a211d90d5.

115 *See* Mark Flannery, US SEC, *Economic Analysis: Providing Insight to Advance the Missions of the SEC and the PCAOB* (Oct 22, 2015), *available at* https://www.sec.gov/news/speech/keynote-address-pcaob-missions-of-sec-and-pcaob.html.

116 *See* OCC, Capital, US Department of Treasury (2019), *available at*

data on each and every business operation, and hence trillions of data sets need to be exchanged.

At the same time, US approaches to client data have been far more laissez-faire than those in Europe, particularly after GDPR but even before its introduction. This has supported the rapid evolution of datafication throughout finance as well as across the economy generally, as acquisition of data combined with analytics has become core in many aspects of the US economy. Unlike the EU, which has a general framework for data protection, the US has developed sector-specific approaches, including for finance. US financial regulation to date has provided a disincentive for BigTechs to evolve into TechFins by entering into financial services:[117] the financial regulatory and compliance burdens have been simply too high and as a result US BigTechs now seem to be seeking to enter finance in the areas of least regulation, perhaps eventually raising issues of shadow banking and regulatory arbitrage.

Thus, as we argued will occur in Europe, the legal and regulatory approaches in the US have been a major driving factor in the evolution of data-driven finance and RegTech. However, they also highlight the potential risks in the context of market dominance and winner-take-all network effects of economies of scope and scale in data. Despite the dominance of US BigTech and US finance, the two have yet to merge. However, given that data, network effects and economies of scope and scale are central to both data and finance, such a confluence of finance and data industries in time seems likely. The main reason why this has not yet happened is the onerous burden of US financial regulation. A light touch regime for data, and a heavy touch one for finance, have so far provided a real disincentive for BigTechs to become TechFins.

Despite this historical trajectory, issues with large tech companies (particularly Facebook) and data protection are beginning to trigger a process of rethinking and may possibly lead to new legislation on data protection, potentially heavily influenced by GDPR. Efforts are also already underway to revise data protection frameworks specifically addressing finance, including at least partially out of the necessity of meeting EU equivalence tests in order to support on-going sharing of data and cross-border usage.

---

https://www.occ.treas.gov/topics/capital/index-capital.html.

[117] Dirk A. Zetzsche, Ross P., Douglas W. Arner & Janos N. Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 14 NYU J. L. & BUS. 393 (2018).

B. China: Leading the World in Data-Driven Finance and TechFin

From a very low base a decade ago, today China has emerged as the world's leading example of digital financial transformation and of the emergence of data-driven finance. It has also emerged as the most developed example of TechFin: the increasing dominance by BigTech in finance.[118]

In China, Alipay (Alibaba) and WeChat Pay (Tencent), as non-interoperable closed payment systems, have demonstrated the disruptive potential of tech-based processes inside financial intermediaries. Alibaba established Alipay in 2004 as a payment method for its ecommerce business. It is now one of the largest mobile wallet providers in the world, along with PayPal and WeChat Pay.[119] The Yu'e Bao money market fund was integrated with the Alipay mobile wallet in 2013.[120] It is now the largest money market fund in the world,[121] having rapidly outgrown the leading US funds, the oldest of which are over half a century old.

WeChat was established as a messaging platform by Tencent in 2011. In 2013, the WeChat Wallet was introduced, and in 2014 was expanded to be able to call and pay for taxis. Cash transfers and in-store cashless payments in some chain stores followed later in 2014.[122] By 2017, 92 percent of respondents to a survey were using mobile payment systems, like WeChat Pay, for retail payments.[123] The rate of uptake and growth has been utterly astounding.

As the use of these two services has skyrocketed, China's central bank, the People's Bank of China ('PBoC'), has subjected them to increasing regulation. Since June 2018, the PBoC has required mobile payment

---

118 *See* Dirk A. Zetzsche, Ross P., Douglas W. Arner & Janos N. Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 14 NYU J. L. & BUS. 393 (2018).

119 *See* D. Bushell-Embling, *Alipay Is World's Second Largest Mobile Wallet*, ComputerWorld Hong Kong (Apr. 9, 2018), *available at* https://www.cw.com.hk/digital-transformation/alipay-world-s-second-largest-mobile-wallet.

120 *See* Eric Mu, Forbes *Yu'ebao: A Brief History of the Chinese Internet Financing Upstart* (May 18, 2014), *available at* https://www.forbes.com/sites/ericxlmu/2014/05/18/yuebao-a-brief-history-of-the-chinese-internet-financing-upstart/#25c898583c0e.

121 *See* Stella Yifan Xie, *World's Largest Money Market Fund Is Shrinking as It Battles Rival on Yields*, WALL STREET JOURNAL (Jan 31, 2019), *available at* https://www.wsj.com/articles/worlds-largest-money-market-fund-is-shrinking-as-it-battles-rival-on-yields-11548934202.

122 *See* S. Millward, *7 Years of WeChat*, TECH IN ASIA (Jan. 21, 2018), *available at* https://www.techinasia.com/history-of-wechat.

123 *See WeChat User & Business Ecosystem Report 2017* (2017), CHINA TECH INSIGHTS, *available at* https://technode.com/2017/04/24/wechat-user-business-ecosystem-report-2017/.

institutions to channel payments through a new centralized clearing house, the China Nets Union Clearing Corporation.[124] This gives the PBoC further control over all payment channels, rather than users directly interacting with payment institutions. The PBoC has also raised the payment platforms' reserve funds ratio to 50 percent from 20 percent, effective April 2018, with the ratio to gradually increase to 100 percent over time, in order to further protect consumers;[125] and has also introduced caps on QR-code-facilitated payments, and on permits to offer barcode payments, to limit fraud.[126]

The experiences of WeChat Pay and Alipay highlight that payments providers should be subject to appropriate proportional regulation, both to address risks and provide a level playing field. However, these experiences also highlight how swiftly and effectively private sector actors can provide digital identification and a flourishing financial ecosystem built upon it. This can be seen most clearly in the recent designation of Ant Financial (Alibaba's affiliate and home to its financial services activities, including AliPay) as a systemically important financial institution in China.[127]

This rapid evolution has occurred in the context of a historically inefficient traditional financial industry combined with a very relaxed approach to data regulation with respect to the acquisition and use of data by both the private sector and the state. The combination – in conjunction with the size and rate of growth of China's economy – has allowed a small number of data firms to increasingly play a leading if not dominant role across China's economy and financial system. These firms are now actively seeking to expand outside of China, in Asia, Europe, the US and beyond.

However, even in China, factors are beginning to constrain these trends. First, stock market and currency turmoil in 2015-2016 led to an increased focus on prudential and other forms of financial regulation. As a result, tech

---

[124] *See* J. Hong, Forbes, *How China's Central Bank Is Clamping Down on the Mobile Payment Industry*, FORBES (Aug. 18, 2017), *available at* https://www.forbes.com/sites/jinshanhong/2017/08/18/how-chinas-central-bank-is-clamping-down-on-the-mobile-payment-industry/#5fa0a13b50be.

[125] *See* Y. Wang, *China Tightens Regulations over Mobile Payment Apps – What's Next for Tencent and Ant Financial?* FORBES (Jan. 3, 2018), *available at* https://www.forbes.com/sites/ywang/2018/01/03/china-tightens-regulation-over-mobile-payment-apps-whats-next-for-tencent-and-ant-financial/#47e526ae7f1d.

[126] *See* S. Jing, *Rules Set for Bar Code, QR Code Payment*, CHINA DAILY (Dec. 29, 2017), *available at* http://usa.chinadaily.com.cn/a/201712/29/WS5a458b89a31008cf16da4193.html; and Xinhua, China Daily, *China Looks for Right Balance between Financial Innovation, Risk* (Dec. 30, 2017), *available at* http://www.chinadaily.com.cn/a/201712/30/WS5a46fd55a31008cf16da4599.html.

[127] Gabriel Wildau, *China to Designate More Financial Groups As 'Too Big To Fail'* FINANCIAL TIMES (Nov 28, 2018), *available at* https://www.ft.com/content/22279e54-f22d-11e8-ae55-df4bf40f9d0d.

firms – both small and large – are facing increasing regulatory burdens.[128] Second, the rapid growth of data-driven finance and the role of new entrants large and small has forced regulators[129] to use RegTech to deal with data on hundreds of millions of transactions and forced tech firms to adopt RegTech to meet their own increasing regulatory compliance burdens (as well as encouraging such firms to lobby regulators to digitize and datafy their systems). Third, most recently, abuses of data by private sector participants are increasingly driving calls to reform data protection,[130] putting in place a general framework for non-state actors similar to that of GDPR.

Looking to China's experience with finance and data, two aspects are most striking: The first is the very widespread acceptance and approval of the extensive and increasingly comprehensive use by the state of data, in ways that would be culturally and politically unacceptable in the US, EU or India (as demonstrated by recent developments relating to privacy and data protection). The second has been a similar level of acceptance of private acquisition and use of data, similar in many ways to that seen in the US. The combination has allowed and even encouraged the state to take an active role in data acquisition and use, most recently in the context of national facial recognition systems and social credit programs. It has also allowed – as in the US – the growth of potential data oligopolies. Unlike the US, however, there has already been a significant confluence of finance and data industries in China, which now leads the world in TechFin. Nonetheless, like the US, the Chinese public and government are increasingly concerned with potential abuses of personal data by the private sector as well as potential negative consequences for innovation and development, resulting in a decision to build both a general data protection framework (as the EU has done with GDPR but likely reflecting a very different cultural environment) as well as a specialized framework for financial services (as the US has already done but is in the process of refining).

The main difference of Europe from China thus lies in data protection and data privacy, with respect to the role of the state and the private sector. All in all when compared to China, the EU legislation differs significantly with regard to the EU's belief in 'ordo liberalism' (i.e. free markets within

---

128 *See* Andrew Meola, *Most Fintech Firms Expect Regulatory Burden to Increase*, BUSINESS INSIDER (Jun 27, 2016), *available at* https://www.businessinsider.com/most-fintech-firms-expect-regulatory-burden-to-increase-2016-6/?r=AU&IR=T.

129 *See* KPMG, *There's a Revolution Coming: Embracing the challenge of RegTech 3.0* (2018), *available at* https://home.kpmg/content/dam/kpmg/uk/pdf/2018/09/regtech-revolution-coming.pdf.

130 *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan 30, 2018), *available at* https://www.cfr.org/report/reforming-us-approach-data-protection.

an organized framework)[131] as well as its strong position on data protection and data privacy, both for commercial and public actors. China also differs dramatically from the US in terms of the views of each society on the role and use of data by government.

C. India Stack: Designing the Infrastructure to Support Digital Financial Transformation, Data-driven Finance and RegTech

India has until very recently lagged well behind the US, Europe and China in finance generally and in the evolution of data-driven finance and RegTech in particular. This however is changing very rapidly as the result of the development and implementation of a comprehensive strategy designed to provide the infrastructure to support digital financial transformation, data-driven finance and RegTech. This strategy – known as India Stack[132] – combines a national system of digital identification, a national digital payments system supporting interoperability across traditional and new payments technologies and providers, an eKYC system to support account opening and use, and a national strategy to use this infrastructure for a range of government and other services such as tax payments, salary payments etc. The combination – as intended – has triggered massive digitization and datafication as well as enabled new entrants and competition, resulting in great increases in financial inclusion, digital financial transformation and innovation, and the emergence of data-driven finance. It has also benefited from RegTech at the core of its design (e.g. eKYC and digital ID systems[133]) as well as supported a revolution in the use of RegTech for compliance and regulatory purposes, particularly in securities markets and payments markets.[134]

India's Aadhaar system is the first level of India Stack.[135] It is operated by the Unique Identification Authority of India (UIDAI) and involves issuing a 12-digit randomized number to all residents on a voluntary basis. Since its initiation, almost the entire population (of approximately 1.3 billion people) has been enrolled and it has been increasingly used to provide access to government services, social benefits, banking and

---

131 *See* Werner Bonefeld, *Adam Smith and Ordoliberalism: on the Political Form of Market Liberty*, Rev. Int'l, Stud. 233 (2013) https://doi.org/10.1017/S0260210512000198.

132 *See* India Stack, *What is India Stack, available at* https://indiastack.org/about/.

133 *See* India Stack, *About eKYC API, available at* https://indiastack.org/ekyc/.

134 *See* Privacy International, *Fintech: Privacy and Identity in the New Data-Intensive Financial Sector* (November 2017), *available at* https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf.

135 *See* India Stack, *About Aadhaar Auth API, available at* https://indiastack.org/aadhaar/.

insurance, and other services. Enrolment to obtain an Aadhaar number is free, and a process of biometric de-duplication seeks to ensure only one number is generated for each individual. The Aadhaar number coupled to biometrics then acts as a proof of identity.[136] The Aadhaar system also provides for a number of methods of updating data. Biometric data can, for example, be updated as children grow, or in the case of accidents or diseases, or as the quality of technology improves.[137]

Aadhaar has proven highly useful for economic and financial inclusion.[138] Aadhaar has made access to financial accounts much easier, thus supporting financial inclusion, and it has enabled digitization of government payments and services, increasing efficiency, decreasing costs and losses due to corruption, and providing a pressing reason for consumers to engage with digital finance. However, there have been a range of real problems in implementation, in particular around privacy and data protection.[139] Aadhaar has been described as 'mass surveillance technology'.[140] It has been subject to a partially successful challenge in the Supreme Court of India[141] and concerns abound as to its susceptibility to misuse and fraud of fingerprinting and iris scanning.[142]

However, Aadhaar has also proven highly beneficial. For example, massive transfer payments previously lost annually through fraud and corruption are now finding their way to the intended recipients, with *The Economist* estimating annual savings as high as US$5 billion.[143] In some states of India, before Aadhaar and associated financial services, up to 45% of government welfare payments were failing to reach their intended

---

[136] *See About Aadhaar*, Unique Identification Authority of India, *available at* http://bit.ly/2HsyzJd.

[137] *See Aadhaar Data* Update, *Unique Identification Authority of India*, *available at* http://bit.ly/2xoDhG4.

[138] *See* Privacy International, *Fintech: Privacy and Identity in the New Data-Intensive Financial Sector* (November 2017), *available at* https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf.

[139] *See* www.stateofaadhaar.in

[140] *See* S. Abraham, R. S. Sharma & B. J. Panda, The Hindu, *Is Aadhaar a Breach of Privacy?*, (March 31, 2017), *available at* http://bit.ly/2BpbVyx.

[141] *See* PTI, *Delji HC Seeks Ayush Ministry's Reply on Plea Against Decision on Aadhaar-based Attendance in Colleges*, TIMES OF INDIA (Mar 10, 2019), *available at* http://timesofindia.indiatimes.com/articleshow/68342358.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst; *see also Puttaswamy (Retd.) & Anor v Union of India & Ors* (Civil) No 494 of 2012.

[142] *See* Cards Tomorrow, *SC Constitution Bench to Begin Final Hearing on Validity of Aadhaar*, LIVE LAW NEWS NETWORK INDIA (Jan. 16, 2018), *available at* http://bit.ly/2p866kw.

[143] *See Indian Business Prepares to Tap into Aadhaar, a State-Owned Fingerprint-Identification System*, THE ECONOMIST (Dec. 24, 2016), *available at* http://econ.st/2FyB0hb.

recipients due to 'leakage'. Indeed, in general terms, difficulties in implementation should not detract from the potential of a national biometrically-based identification system to underpin a digital financial ecosystem. Digital ID, however it is established and validated, is necessary to provide a solid foundation for the other parts of the ecosystem.

Such a comprehensive digital financial ecosystem has the potential to transform governance and delivery of services and result in economic gains that can be used to fund investments in education, health, roads and other infrastructure.[144] Such an ecosystem can transform the payment of government benefits, dramatically reducing losses due to corruption, and should be able to allocate credit in such a way that SMEs, the principal employers of people in most countries, can thrive.

Unlike China and the US, India – despite the size of its rapidly evolving market – has not yet seen the emergence of BigTech, TechFin or even massive financial conglomerates of the sort common in the US or Europe. One reason may be that, in implementing the centralized strategy of an India stack, various state arms play a particularly strong role in financial market infrastructure.[145] In turn, private actors find room for new services in particular in the field of collateral applications rather than financial core infrastructure such as digital identity and bank account services. Or it may simply be that India is at a lower stage of financial and economic development and that developments in India will move very rapidly as has been the case in China, now that the core elements necessary to support digital financial transformation are in place.

D. Comparative Lessons

India's strong centralized agenda to support digital financial transformation is certainly demonstrating the potential of approaching data-driven finance strategically – which is the truly transformative potential of RegTech.[146] China's path to data-driven finance has been entirely different, and emerged from the largely unfettered market activities of a small number of major tech firms, often with close state relations, but without any overriding

[144] *See* Douglas W. Arner, Ross P. Buckley & Dirk A. Zetzsche, Alliance for Financial Inclusion, *FinTech for Financial Inclusion: A Strategy for Digital Financial Transformation* (Sep. 2018), *available at* https://www.afi-global.org/publications/2844/FinTech-for-Financial-Inclusion-A-Framework-for-Digital-Financial-Transformation.

[145] *See* Privacy International, *Fintech: Privacy and Identity in the New Data-Intensive Financial Sector* (November 2017), *available at* https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf.

[146] *See* Arner, Barberis & Buckley, RegTech, *supra* note 2, at 4.

national strategy prior to 2015-2016.[147]

With data regulation the US and China have taken far more laissez-faire approaches than Europe or India, as India largely followed EU data protection approaches prior to GDPR. In both the US and China, free transferability of data has allowed acquisition of large pools of data, reflected in the emergence of a small number of very large firms based on network effects and economies of scope and scale for data. Both the US and China however have experienced negative as well as positive results from this approach and both are considering alternatives, including the EU approach of GDPR.

Like India, and increasingly in China, Europe has given the state an important role in data. In Europe, this is in regulating strictly the use of data by governments and the private sector; in China it is the wide use of data by government in all its activities; and in India it is the design of systems to encourage digitization and datafication while balancing efficiencies and risks with data protection and privacy considerations. Sectoral needs such as those of financial regulators to better control systemic risks, or enhancing the service level of European banks, or ensuring privacy in a world dominated by data-driven firms have determined the path taken, not some overarching government policy. By contrast, until very recently, both the US and Chinese systems have been characterized by a highly laissez faire approach to end-user data in the private sector.

IV. POLICY PERSPECTIVES: TOWARDS DATA-DRIVEN FINANCE

A. A Big Bang Theory

The EU experience highlights how, as financial systems digitize, it is necessary to carefully consider approaches to financial regulation, cybersecurity, data protection, digital identity and competition. The approaches taken in different jurisdictions – and the resulting role of RegTech – will be driving forces in financial and economic development and innovation in the 21st century.

As discussed in Part II, financial intermediaries have often collected large amounts of data from and about their customers, over long periods of time. However, in many cases, these data were not used effectively, because

[147] The very rapid growth in Ant Financial and other firms prompted the People's Bank of China to take steps to slow down developments and better manage potential risks in 2015-16. *See* Weihuan Zhou, Douglas W. Arner & Ross P. Buckley, *Regulation of Digital Financial Services in China: Last Mover Advantage*, 8 TSINGHUA CHINA L. REV. 25 (2015).

they have been restricted to certain business units, lines, products or silos within individual firms.[148] 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.

However, unlike the financial regulatory reforms which underpin not only digitization but also datafication through the application of analytics to massive amounts of data – providing the impetus for data driven finance in Europe's traditional financial industry as well as the rapid evolution of RegTech both by the industry and regulators – GDPR instead 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).

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,[149] 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 two separate rulebooks (or in Europe's case four separate rulebooks) 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, with important implications for RegTech

Thus, while regulation places limits on data-driven finance and RegTech it also drives both 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.[150] As

---

148 *See* da Silva & Goetz von Peter, *supra* note 76 at 21.

149 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 analyzed and applied effectively.

150 *See generally* EUROPEAN BANKING AUTHORITY, REPORT ON THE PRUDENTIAL

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 such as MiFID 2, GDPR, PSD 2 and eIDAS. It is the combination of regulatory approaches and policies which are and will continue to push forward data-driven finance and RegTech in the EU. Indeed, we suggest that over time 2018 will come to be viewed as a Big Bang in both RegTech and the evolution of data-driven finance in Europe.

As other jurisdictions around the world are increasingly forced to consider the interaction of financial regulation, data protection, and cybersecurity in the context of their own cultural and political environments, the experience of the EU with this Big Bang will provide major lessons for policy and regulatory choices. This will also be the case as jurisdictions consider the relationship of financial regulation, data protection, and cybersecurity with competition / antitrust policy and regulation. This topic however is beyond the scope of this paper.

B. The Building Blocks of the Road to RegTech

This confluence of regulatory reforms has shaped not only the evolution of data-driven finance (below section C.), but also the development and use of RegTech solutions in Europe. We suggest six initial conclusions in relation to the future evolution of RegTech before ending by considering policy lessons around the transformation to data-driven finance.

First, RegTech is not, or should not be, the simple transposition of existing analogue processes into a digital context, but requires instead a reinvention of these processes. The datafication of processes requires a Digital Due Diligence approach which divides processes into tiny steps that can be captured in a binary and check-the-box fashion. This then facilitates default and override hierarchies that must be carefully considered and implemented.

Second, the adoption of RegTech will require a readjustment of accountability and liability rules. Where the lines are to be drawn is neither obvious nor simple. An overly friendly approach to technology exposes clients and the financial system to the risk of tech vulnerabilities, while an overly strict approach renders unnecessarily difficult and expensive the management of financial intermediaries. A possible approach may be one that assesses the diligence applied to software and data use, management and processing decisions, and treats leniently those arising from care and

---

RISKS AND OPPORTUNITIES ARISING FROM FINTECH (3 July 2018); EUROPEANS BANKING AUTHORITY, REPORT ON THE IMPACT OF FINTECH ON THE INCUMBENT CREDIT INSTITUTIONS' BUSINESS MODEL (6 July 2018)

diligence – something akin to the business judgement rule regarding the liability of corporate directors.

Third, the nature of supervision will change as a result of RegTech. Data-driven supervision is a different skill than more traditional form-based approaches. Accordingly, while the judgement calls may be similar, the information these will be based on will be far more granular and up-to-date, and a different skill set may well be necessary for RegTech-based 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, the rise of RegTech will lead to fewer human resources needed in banks for client 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. Most jurisdictions face human resourcesshortages in this area. Implementing a RegTech strategy thus requires a more comprehensive approach including academia and educational programs, in general.

Fifth, RegTech does not abolish risks. Rather, some risks to which we are well accustomed will be replaced by new risks. For instance, human-based operational risk, one of the major capital costs since the 2008 Crisis, should decrease, whereas cybersecurity and tech risks will increase. Further, in our view, antitrust risks and the risks for markets resulting from extremely swift transmission of information will increase and require further investigation. We address this aspect further, at part IV.C.

Sixth, as RegTech develops, financial intermediaries will need to re-consider their risk budgets and capital allocations. Reviewing risk models has long been a challenge. Unique risk models have created information asymmetries, leading some capital markets to penalize banks with advanced risk models by imposing discounts on the disclosed book values. For this reason, standardization of risk models is on the regulatory agenda. However, this standardization may bring with it a loss of innovation and increased systemic risk since standardization of risk models will likely lead to standardized business models and strategies, as arguably occurred in the 2008 Crisis and which has become a core focus of macroprudential regulation. However, RegTech enables supervisors to assess, for the first time, the impact of firm-specific risk models by transferring the underlying data sets into the supervisor's risk modelling systems and then stress testing against certain occurrences. So RegTech should improve supervision and reduce market concerns about advanced, bespoke risk models. For this reason, RegTech could render unnecessary the standardization of risk models, and replace it with the disclosure of supervisory assessments of the projected outcomes of bespoke risk models.

C. 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 RegTech, 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 particularly in the context of 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 data regulation 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. 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 as to the financial law's objectives and hence the remits of supervisors: Where the power is in the data we would recommend financial regulators to accept that the new systemic risk stemming from concentration of data in the hands of a few technology firm complements the old 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 favor of financial customers. The measures that result may well look similar to existing antitrust approaches, based on a financial law rationale: systemic risk.

V. CONCLUSION

In this paper we have argued that a series of clearly motivated but uncoordinated projects played a crucial role in shaping 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. 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 this regard the EU presents an interesting and very much still evolving case study, relevant to every other jurisdiction in the world. In the EU, what has been necessary to take the road to data-driven finance and RegTech 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 ('EBA')) 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 – outside of select jurisdictions such as the UK und Luxembourg – would have been possible in the practice of financial supervision.

Looking forward, it is now clear that Europe's experience with its four 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 Europe 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 customer 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 in developed markets and that this process is likewise happening very rapidly in emerging and developing markets. As a result, use of technology for compliance, monitoring, enforcement, and system design in financial regulation will continue to

increase. There will be particular challenges for regulators and supervisors in managing the process but also opportunities to consider how to use RegTech to design better systems to achieve regulatory objectives. From this standpoint, jurisdictions are already considering how to shape the evolution of RegTech through digitization, datafication and systems design, in a process that will only increase in importance going forward. In addition to the important benefits, the transition of data-driven finance and RegTech also brings new risks, in particular in the context of cybersecurity, technology and data protection.

The second clear lesson is that each society must grapple with its own approach to data and its role in their future. These discussions will involve not only questions of finance and data regulation but also of social regulation and competition / antitrust regulation. As has been shown in this paper, different societies can have very different views on this issue and on the sorts of governance and economic systems they wish to see in their futures. These issues however 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 in the use of data by governments, 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 (particularly those with a clear RegTech strategy) 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. We would argue that most jurisdictions will need both a general data regulation framework 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.

***

Address

European Banking Institute eV.

Mainzer Landstrasse 251

60326 Frankfurt am Main

Germany

For further information please visit our website www,ebi-europa.eu or contact us at info@ebi-europa.eu

www.ebi-europa.eu

The European academic joint venture for research in banking regulation

www.ebi-europa.eu