Technological Transformations in the Financial Sector: Principles for *Lex Specialis, Lex Generalis* and their Interrelationship

Iris H-Y Chiu*

Abstract

Technological transformations often affect business sectors and not just finance. Hence, financial regulators have to grapple with the aptness of regulatory designs that deal with these technological phenomena, as they are not confined to being specialist and sectoral, but generate risks of a cross-sectoral nature. Regulators are developing specific financial regulation regarding technological phenomena and risks, a development we call *lex specialis* in this article. This article argues that while *lex specialis* is often warranted by precise financial regulatory objectives, there are useful consistency benefits and governance standards that can be designed at a cross-sectoral level. In this manner, financial regulators can learn from and work with regulators that curate cross-sectoral regulation, we call *lex generalis* in this article. Financial regulators seeking a holistic perspective affecting their own stewardship of regulatory objectives cannot ignore other needs in technological governance. Hence, financial and other regulators need to be prepared for embracing the dynamic landscape of interaction between *lex specialis* and *lex generalis*. Regulators can benefit from formalised coordinative and cooperative structures across sectors which cater for regulators' needs in knowledge-building and governance thinking. Such structures can be elevated to the international level where systemically important Bigtechs are concerned, for supervising the risks they pose to finance, economies and societies.

1. INTRODUCTION

The last decade since the end of the 2007-9 global financial crisis bears witness to the rise of many technological transformations in the financial sector,[1] including: (a) front end financial business interfaces such as "appification";[2] (b) the emergence of new types of financial services based on data harvesting and analysis (beyond traditional models where proprietary relationship-based information prevailed), such as on crowdfunding platforms; (c) increasing offerings of accessible and automated types of financial intermediation including loan, insurance underwriting and investment management and (d) the building out of financial service businesses on virtual or third-party infrastructure such as the cloud. Many of these transformations, conveniently dubbed as the rise of financial technology (fintech), have been welcomed by regulators as they offer new opportunities for financial

* Iris H-Y Chiu, Professor of Corporate Law and Financial Regulation, University College London.

[1] Arnaud Boot et al., "Fintech: What's Old What's New" (2021) 53 J. Financial Stability 100836.

[2] See generally, Accenture, "Managing the Growing Appification of Business" (last modified 19 December 2013), online (pdf): *Accenture* <https://www.accenture.com/t20150523T130138__w__/be-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_6/Accenture-13-3975-Appification-POV.pdf>; The "appification" of stock trading portals such as provided by Robinhood is discussed in Tony Klein, "A Note on GameStop, Short Squeezes, and Autodidactic Herding: An Evolution in Financial Literacy?" (2021) Queen's University Belfast Working Paper Ver. 2, online: *Social Science Research Network* <https://ssrn.com/abstract=3845722>.

efficiency and inclusion.[3] Their potential for competitive disruption and the new risks they generate have also been subject to regulatory scrutiny, such as in programmes of regulatory sandboxes and regulators' consultation and reform discussions.[4]

Many of these technological revolutions do not only affect the financial services industry but are potentially deployable in other business sectors causing different degrees of transformation and disruption. Hence, different sectors may experience similar risks entailing from increased deployment of digital technologies and virtual business mobilisation. Platform technologies build multisided markets not only for the supply and demand sides in finance, but also for other goods and services such as hired chauffeuring,[5] accommodation services,[6] parking services[7] and used consumer goods.[8] Artificial intelligence systems can be used to automate, to more or less intelligent degrees, various front-end, operational and back-end roles in many business sectors.[9] The migration from ever-expanding local servers to cloud infrastructure is occurring in many sectors including finance.[10] Financial services businesses, along with many other private sector entities, as well as public sector entities, face heightened needs for combatting cybersecurity risks. In this manner, we observe that not only do sector-specific regulatory bodies embark on law reform to address the implications of technological transformation, but also some regulatory reforms take on a "cross-cutting" nature in order to address common problems and risks across sectors, such as the EU *Digital Services Act*,[11] that deals with all platform businesses and the proposed EU Regulation of Artificial Intelligence Systems.[12] These "cross-cutting" regulations sometimes also provide for the creation of new cross-sectoral oversight bodies, such as the proposed European Artificial Intelligence Board, that would support the cooperation between Member State regulators and the Commission's policy work and implementation expectations.

---

[3] George Okello, Candiya Bongomin & Joseph Mpeera Ntayi, "Mobile Money Adoption and Usage and Financial Inclusion: Mediating Effect of Digital Consumer Protection" (2020) 22 Digital Policy, Regulation & Governance 157.

[4] Deidre Ahern, "Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon" (2021) European Banking Institute Working Paper No. 102, online: *Social Science Research Network* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3928615>; see also Dirk A. Zetzsche et al., "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation" (2017) 23 Fordham J. Corporate & Financial L. 31; see e.g. the Financial Stability Board's interest and work in Fintech reflects members' interests and policy needs, Financial Stability Board (FSB), "FinTech" (last modified 5 May 2022), online: *Financial Stability Board* <https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech/>.

[5] Such as Uber and Lyft.

[6] Such as AirBnB and Vrbo.

[7] Such as JustPark.

[8] Such as eBay.

[9] See generally, Iris H-Y Chiu & Ernest W.K. Lim, "Technology vs Ideology: How Far will Artificial Intelligence and Distributed Ledger Technology Transform Corporate Governance and Business?" (2021) 18 Berkeley Bus. L.J. 1.

[10] Jean-François Blanchette, "Introduction: Computing's Infrastructural Moment" in Christopher S. Yoo & Jean-François Blanchette, eds., *Regulating the Cloud* (Cambridge, Massachusetts: MIT Press, 2015) (see chapter 1).

[11] EC, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)* [2022] OJ, L 277/1 [EU DSA].

[12] European Commission, "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence" (last accessed 8 June 2023), online: *European Commission* <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>.

There is arguably a need to consider the coherence and holistic mapping of "cross-cutting" regulatory policy, which in this article is called "*lex generalis*", with sector-specific regulatory policy and objectives, which in this article is called "*lex specialis*." This article focuses only on *lex specialis* in finance. Contradictions or incoherence between *lex generalis* and *lex specialis* can produce heightened legal risks for firms. The implication of multiple regulators' enforcement jurisdictions can also bring about multiple jeopardy. Clarity for regulators' remits also benefits their determination of priorities and deployment of resources. There is also a need for regulators to consider holistically how *lex generalis* or *lex specialis* can enable innovations that promote market choice while also governing them in a manner that mitigates regulatory arbitrage, while being attentive to new risks that may arise.

This article discusses developments in *lex generalis* and *lex specialis* that affect the financial sector broadly, in order to tease out some high-level principles for governing the interrelationship between *lex generalis* and *lex specialis*. To do so, this article draws examples from the following major technological developments: platformisation or multi-sided digital/online markets for finance; the development of artificial intelligence systems for financial services and other operations, particularly in machine learning based on advancements in data analytics; the adoption of virtual or cloud-based infrastructure for financial services entities in larger or smaller degrees; interoperability in financial services across different entities and the rise in importance of cybersecurity. These developments have almost unsparingly affected financial services businesses across the sector. As the approach in this article is towards articulating high-level principles for the interrelationship between *lex generalis* and *lex specialis* applicable to technological transformations of the financial sector, this article will not comprehensively focus on any particular area of technological transformation in detail in order to make specific substantive proposals.

Further, the article omits two highly disruptive technological phenomena: the use of distributed ledger technology in financial services or by financial entities, as well as the development of non-fiat money denominated products and services that engage financial interest, in the sense that speculation or expectation of gain may be implicated. On the former, many different financial institution incumbents have engaged in pilot projects, ranging from securities clearing and settlement to multipartite fund-raising transactions and cross-border banking. Distributed ledger technology (DLT) potentially changes the roles and responsibilities of "nodes" in the relevant financial system, entailing potential significant regulatory policy disruptions.[13] In this manner, the issues arising from DLT adoption go beyond the boundaries and interrelationships between *lex generalis* and *lex specialis*, and threaten to redraw regulatory boundaries altogether.[14] DLT transformations warrant a separate discussion altogether. However, empirical evidence has documented many financial entities' disappointment with the lack of efficiency and other savings from reframing financial transactions/services within DLT frameworks.[15] This means that the need

[13] Dirk A. Zetzsche et al., "DLT-based Enhancement of Cross-Border Payment Efficiency – A Legal and Regulatory Perspective" (2021) 15 L. & Financial Markets Rev. 70.
[14] Jason Grant Allen & Rosa M. Lastra, "Border Problems: Mapping the Third Border" (2020) 83 Mod. L. Rev. 505.
[15] Martha Muir, "Case for blockchain in financial services dented by failures" (30 December 2022), online: *Financial Times* <https://www.ft.com/content/cb606604-a89c-4746-9524-e1833cd4973e>.

for overhauling whole regulatory policies for DLT-based financial transactions, services or products remains highly debatable.

In relation to non-fiat money denominated products and services that engage with people's speculative interests, such as in relation to crypto-token investments,[16] stablecoins[17] and decentralized finance (DeFi),[18] there is ongoing debate relating to whether new regulatory regimes altogether are justified,[19] or otherwise.[20] Whether non-fiat money denominated "finance" should be recognised as "mainstream" via regulatory policy is highly contested and attracts a different discussion altogether. Hence, this article focuses on technological transformations of mainstream finance in terms of fiat money-denominated financial activities that are engaged by financial institution incumbents and fintech entities.

Section A discusses the policy drivers for *lex specialis* in financial regulation responding to certain technological transformations. This section explains why regulators perceive the need to articulate special treatment in order to ensure that existing regulatory objectives are met. This section discusses examples in platformisation, open banking and the regulation of financial institutions' information technology systems and procurement. Although *lex specialis* is largely a response to the need to protect existing regulatory objectives, regulators often engage in complex and multiple-objective considerations. Further, it is also observed that many *lex specialis* regimes are meta-regulatory in nature with scope for transitioning into more precise substantive regulatory policy.

Section B argues that *lex generalis* is usually driven by regulatory objectives that overlap with but exceed financial regulators' remits. In this manner, the institution of such *lex generalis* is usually underpinned by multiple objectives and may present challenges in relation to coherence and clarity in regulatory expectations and experience for the regulated entities. The section looks in particular at the proposed EU regulation of artificial intelligence systems as a key example where the financial sector would be equally affected by *lex generalis* and *lex specialis*. The Section also discusses how regulatory agencies' remits and architecture may be affected.

---

[16] See e.g. Jonathan Rohr & Aaron Wright, "Blockchain-based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets" (2019) 70 Hastings L.J. 463 on the characterisation debates in the US; see also Philipp Hacker & Chris Thomale, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law" (2018) European Company & Financial L. Rev. 645 on the EU.

[17] FSB, "Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements: Consultative report" (11 October 2022), online: *FSB* <https://www.fsb.org/2022/10/review-of-the-fsb-high-level-recommendations-of-the-regulation-supervision-and-oversight-of-global-stablecoin-arrangements-consultative-report/>; Edoardo Martino, "Regulating Stablecoins as Private Money between Liquidity and Safety. The Case of the EU 'Market in Crypto Asset' (MiCA) Regulation" (2022) Amsterdam Center for Law & Economics Working Paper No. 2022-07, online: *Social Science Research Network* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4203885>.

[18] Iris H-Y Chiu, "Regulating Crypto-finance: A Policy Blueprint" (2020), University College London Working Paper No. 570/2021, online (pdf): *European Corporate Governance Institute* <https://ecgi.global/sites/default/files/working_papers/documents/chiufinal.pdf>; Dirk A. Zetzsche, Douglas W. Arner & Ross P. Buckley, "Decentralised Finance" (2020) 6 J. Financial Regulation 172.

[19] See e.g. Iris H-Y Chiu, *Regulating the Crypto-economy: Business Transformations and Financialisation* (Oxford: Hart Publishing, 2022) [Chiu, "Regulating"].

[20] Hilary J. Allen, *Driverless Finance* (Oxford: Oxford University Press, 2022) (see chapters 5 and 6).

Section C then turns to ask if "Bigtech" in finance poses challenges that require special approaches in *lex generalis* and *lex specialis* working together to mitigate a variety of different risks. Although there is potentially a case for *sui generis* "Bigtech" regulation if they become systemically important global financial supermarkets, this seems not to have taken place so far in mature financial jurisdictions, especially in the West.[21] However, even if the West may not grapple with the equivalent of an "Ant Financial" phenomenon, new consolidations in the financial sector based on data-driven or digital synergies could warrant regulators' attention.[22] This section also evaluates how Bigtech governance highlights the necessary interrelationship between *lex generalis* and *lex specialis* for financial regulators. Section D concludes.

2. THE DEVELOPMENT OF TECHNOLOGICALLY-RESPONSIVE *LEX SPECIALIS*

Although financial regulators have purported to be "technologically neutral" and apply an approach of "same activity, same risks, same rules"[23] or "same risks, same regulatory outcomes,"[24] Brownsword has argued that the law's relationship with technological changes is not merely one of maintaining "coherentism."[25] Technological changes that disrupt financial intermediation in terms of the nature of products, delivery of services, introduction of new intermediation entities or creation of new types of markets could give rise to issues of fit with existing institutional frameworks as well as regulatory arbitrage.[26] I have elsewhere argued that the institutional underpinnings of financial regulatory regimes shape

---

[21] FSB, "FinTech and Market Structure in the COVID-19 Pandemic" (21 March 2022), online (pdf): *FSB* <https://www.fsb.org/wp-content/uploads/P210322.pdf>; Barry Eichengreen, "Financial Regulation in the Age of the Platform Economy" (2021) 24 J. Banking Regulation 40, online: *Springer Link* <https://doi.org/10.1057/s41261-021-00187-9>.

[22] Dirk A. Zetzsche et al., "Digital Finance Platforms: Toward a New Regulatory Paradigm" (2020) 23 U. Pa. J. Bus. L. 4 [Zetzsche et al., "Paradigm"].

[23] FSB, "International Regulation of Cryptoasset Activities: A Consultation" (11 October 2022), online (pdf): *FSB* <https://www.fsb.org/wp-content/uploads/P111022-2.pdf>; Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), "30 Recommendations on Regulation, Innovation and Finance" (16 December 2019), online (pdf): *European Commission* <https://commission.europa.eu/system/files/2019-12/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf>; European Commission, *Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU*, [2020] OJ, COM 591, online: *European Commission* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0591>.

[24] Jon Cunliffe's preferred "same risks, same regulatory outcomes" which bears some similarity to the above; see Jon Cunliffe, "Some Lessons from the Crypto Winter" (12 July 2022), online: *Bank of England* <https://www.bankofengland.co.uk/speech/2022/july/jon-cunliffe-speech-on-crypto-market-developments-at-the-british-high-commission-singapore>.

[25] Roger Brownsword, *Law, Technology and Society: Reimagining the Regulatory Environment* (Oxford: Routledge, 2019) at 191-196.

[26] Tom C.W. Lin, "Infinite Financial Intermediation" (2015) 50 Wake Forest L. Rev. 643; Johan Bouglet, Ghislaine Garmilis & Olivier Joffre, "Challenges and Opportunities for Crowdfunding in Emerging Markets: An Ethical Perspective" in Duc Kuong Nguyen, ed., *Handbook of Banking and Finance in Emerging Markets* (Cheltenham: Edward Elgar, 2022) (see chapter 26); see Iris H-Y Chiu, "An Institutional Account of Responsiveness in Financial Regulation- Examining The Fallacy and Limits of 'Same Activity, Same Risks, Same Rules' as the Answer to Financial Innovation and Regulatory Arbitrage" (2023) Symposium volume for the Computer Law and Security Review, forthcoming [Chiu, "Institutional"]; broadly explained as the exposure of gaps in incomplete regulatory contracts, see Heikki Marjosola, "The Problem of Regulatory Arbitrage: A Transaction Cost Economics Perspective" (2021) 15:2 Regulation & Governance 388.

financial regulators' responsiveness to technological changes, including whether regulators would develop specialist regimes for technologically-transformed financial services and intermediation.[27] In this section I examine the drivers for *lex specialis* without delving into the dimension of institutional context, but I develop complementary arguments with earlier work, at a level of broader normative application. These drivers for *lex specialis* are based on financial regulators' objectives.

(a) Enabling Competitive Markets

An important regulatory objective that financial regulators have pursued in the EU and UK is that of enabling competition in financial services markets. The UK Financial Conduct Authority has an explicit objective to promote competition,[28] as competitive markets can improve consumer choice. The EU's economic and policy objective is to foster a Single market in financial services, whether relating to banking, insurance, investment or payment services. This objective facilitates supply side entry into many national markets in the EU, and is also aimed at improving choice for the demand side. In this manner, encouraging competition is complementary to the Single market objective.

This section argues that policy-makers' pro-competition stance has led to the introduction of *lex specialis* that *enables* innovations to be mobilised. Such *lex specialis* treats innovations in a regulatory category of their own so as to legitimise their activities without extending incumbents' regulatory regimes in full. *Lex specialis* is able to provide for an enabling regulatory regime for such innovations, subjecting them to different designs in terms of governance and obligations, as these may be more proportionate to the cost/benefit profiles of such innovations. In particular, *lex specialis* arguably reflects policy-makers' buy-in of the benefits of certain innovations, particularly in relation to financial inclusion, consumer choice and market competition. In this manner, *lex specialis* for certain financial innovations is distinguished from: (a) regulatory regimes for other incumbents' financial services which may share certain similar functions; and (b) general technological governance and regulation, such as over digital data, technological interoperability or platforms more broadly.

First, in the absence of such *lex specialis*, the application of "existing same rules," which have been developed with incumbent industrial structures in mind, would be deterring to new entrants. Powerful incumbents in the financial sector often offer bundled lines of financial services, such as banking institutions that offer a bundle of deposit-taking, payment services and credit.[29] Many systemically important financial institutions today are financial supermarkets with mega footprints in almost every line of wholesale and retail financial sector business.[30] Disruptive technological transformations in finance often pose challenges in relation to "unbundling" one or two aspects of incumbents' bundled business

---

[27] Chiu, "Institutional", *supra* note 26.
[28] *Financial Services and Markets Act* (UK), 2000, s. 1E (amended 2012) [*FSMA*].
[29] Dan Awrey, "Unbundling Banking, Money, and Payments" (2022) 110 Geo. L.J. 715.
[30] Such as JP Morgan, HSBC, Citigroup, etc.; see work done by the Financial Stability Board and Basel Committee, FSB, "Global Systemically Important Financial Institutions (G-SIFIs)" (last accessed 9 June 2023), online: *FSB* <https://www.fsb.org/work-of-the-fsb/market-and-institutional-resilience/global-systemically-important-financial-institutions-g-sifis/>.

models. For example, many fintechs aim at making payment interfaces more user friendly, hosted on smartphones and other mobile devices, therefore unbundling certain aspects of payment services from account-based banking services. Further, fintechs such as MoneyBox or Money Dashboard aim at helping users to visualise their financial positions and to make financial plans and budgets. Fintech competition has driven beneficial changes in the payment services market in relation to cost and speed of payments, remittances and has also mobilised small retailers' access to cashless payment systems.[31] To impose the full gamut of bank regulation on fintechs would be disproportionate as fintech businesses are often smaller and not balance sheet-based. These characteristics distinguish the nature of risks generated by such fintechs from industry incumbents, and makes a stronger case for enabling forms of *lex specialis* for fintechs, rather than the extension of existing same rules. The extension of existing bank regulation would only allow incumbents to shut out new entrants in the name of preventing regulatory arbitrage. Regulatory arbitrage, however, should be understood as a phenomenon that occurs due to gaps in the regulatory "contract,"[32] and need not be negatively associated with regulatory evasion. Further, innovations that deliver effectiveness in financial services while minimising existing burdens or cost can be seen to be offering potential efficiency lessons. The development of *lex specialis* neutralises negative impressions of "regulatory arbitrage" and legitimises new developments that can be socially beneficial. In this manner, this section argues that there is tight coupling between regulators' motivations to *enable* motivations and their introduction of *lex specialis*.

(i) Enabling competitive markets in payment services – an example

The EU's Payment Services Directive 2015 explicitly recognises a payment services sector as distinct from the banking sector, and different types of service providers that are independent of banking services.[33] Enabling forms of *lex specialis* include regulatory standardisations that facilitate new supply-side entrants to come to market. The UK's Open Banking Initiative institutes a new regulatory agency to oversee the development of standardised "application programming interfaces" (API) for payment services.[34] These API standards provide a public good that allows for financial information sharing amongst whitelisted financial services providers, including fintech firms. In this manner, fintech firms are enabled to compete on a level playing field with incumbents who could otherwise reject sharing customer information or erect high barriers to do so.

The Open Banking Initiative is particular to fintechs, and does not address the broader issue of commercial data-sharing or digital interoperability. There is however a wider need across

---

[31] Prove, "Six Ways FinTech is Helping Small Business Owners Meet Cash Flow Challenges" (7 September 2021), online: *Prove* <https://www.prove.com/blog/six-ways-fintech-helping-small-business-owners-meet-cash-flow-challenges>; Wharton, "6 Ways Fintech Is Helping Small Business" (11 June 2019), online: *Wharton* <https://online.wharton.upenn.edu/uncategorized/fintech-is-helping-small-business/>.

[32] Marjosola, *supra* note 26.

[33] Alan Brener, "EU Payment Services Regulation and International Developments" in Iris H-Y Chiu & Gudula Deipenbrock, eds., *The Routledge Handbook of Financial Technology and Law* (Oxford: Routledge, 2021) (see chapter 9).

[34] Andreas Kokkinis & Andrea Miglionico, "Open Banking and Libra: A New Frontier of Inclusion for Financial Services in payment Systems" (2020) Singapore J. Leg. Studies 601; Christopher C. Nicholls, "Open Banking and the Rise of FinTech: Innovative Finance and Functional Regulation" (2019) 35 B.F.L.R. 121.

sectors for such digital seamlessness and technological interoperability, for example, in relation to the internet of things. Such enabling regulation would need to address data-sharing more generally, privacy concerns as well as security standards, bearing in mind the difficulties of coordination amongst a wide scope of private and public sector parties and agencies that would be involved. The EU is progressing with an open but governed architecture for data-sharing under the *Data Governance Act* and *Data Act* respectively.[35] In this manner, the EU's Payment Services Directive and the UK's Open Banking Initiative have created *lex specialis* ahead of the broader generalist debate and reforms. These initiatives are in no small part due to the perceptions of innovative benefits that financial regulators particularly wished to mobilise.

(ii) Enabling competitive markets in small business fund-raising - an example

Another example is the development of *lex specialis* for loan and equity-based crowdfunding platforms in the UK and EU. In the absence of *lex specialis*, loan-based crowdfunding could be pre-empted by bank and consumer credit regulation, while equity-based crowdfunding could run afoul of securities regulation above the stipulated minimum levels of exemptions. Empirical evidence shows the importance of access to crowdfunding platforms for small businesses to meet their fund-raising needs.[36] The retail peer-to-peer lending market is also important for financial inclusion in relation to access to credit.[37]

The UK's introduction of a regulatory framework for crowdfunding platforms in 2014 legitimises platforms' activities in a tailor-made *lex specialis* applicable to them.[38] In this manner, existing regimes regarding consumer credit, securities regulation or collective investment scheme regulation (which could apply if platforms diversify investors' contributions and curate their investments into portfolios of loans in peer-to-peer lending, for example) would not be applicable. *Lex specialis* also allows regulators to allocate

---

[35] European Commission, "Commission welcomes political agreement to boost data sharing and support European data spaces" (30 November 2021), online: *European Commission* <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6428>; European Commission, "Data Act: Commission proposes measures for a fair and innovative data economy" (23 February 2022), online: *European Commission* <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113>.

[36] Victor Tiberius & Raoul Hauptmeijer, "Equity Crowdfunding: Forecasting Market Development, Platform Evolution, and Regulation" (2021) 59 J. Small Bus. Management 337; Peter Chapman, "Crowdfunding" in Jelena Madir, ed., *Fintech: Law and Regulation* (Cheltenham: Edward Elgar, 2019) (see chapter 3).

[37] See e.g. Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, "The Rise of Techfins: Regulatory Challenges" in Jelena Madir, ed., *Fintech: Law and Regulation* (Cheltenham: Edward Elgar, 2019) (see chapter 13) [Zetzche, Buckley & Arner, "Techfins"]; Jon Frost et al., "BigTech and the changing structure of financial intermediation" (2019) 34:100 Economic Policy 761 (on increased inclusiveness of platform and Bigtech lending); but see warnings regarding predatory lending, Allen, *supra* note 20 (see chapter 7); Kristin Johnson, Frank Pasquale & Jennifer Chapman, "Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation" (2019) 88 Fordham L. Rev. 499; Bongomin and Ntayi (2020) discuss the inclusive benefits of mobile money transfer systems; Tan discusses the inclusive benefits of online trading but warn against the dangers of predatory allure, see Gordon Kuo Siong Tan, "Democratizing Finance With Robinhood: Financial Infrastructure, Interface Design and Platform Capitalism" (2021) 53:8 Environment & Planning A.: Economy & Space 1862.

[38] FCA, "COBS 4.7 Direct offer financial promotions" (last modified 6 January 2021), online: *FCA* <https://www.handbook.fca.org.uk/handbook/COBS/4/7.html> [FCA Handbook]; but see amendments at FCA, "Strengthening our Financial Promotion Rules for High-Risk Investments and Firms Approving Financial Promotions" (August 2022), online (pdf): *FCA* <https://www.fca.org.uk/publication/policy/ps22-10.pdf> (in force from 1 December 2022).

regulatory duties and responsibilities in a different manner than under other existing regulatory regimes. EU regulation was also introduced in 2020 adopting similar balances in policy approach.[39] By adopting *lex specialis*, financial regulators are able to articulate the balance of objectives they wish to achieve, such as enabling innovation and competition, alongside ensuring investor protection, and to those ends, engage with governance and responsibility distributions and designs, without the "baggage" of applying existing regulatory regimes.

Regulators' enabling objectives in *lex specialis* are reflected in their proportionate approaches to duties and obligations imposed on participants in the online crowdfunding market. Further, such regulation can be relatively skeletal or meta-regulatory to begin with,[40] meaning that financial regulators provide only broad outlines of conduct expectations, leaving the "newly" regulated entities to develop internal and market practices. The Financial Conduct Authority's (FCA) initial regulatory framework in 2014 had only a few prescriptive prudential and consumer protection provisions for platforms, such as ensuring that retail customers have received mandatory advice and to impose a cap on their investment based on their net disposable assets. These existed alongside meta-regulatory provisions leaving platforms to inform their users of the extent of their due diligence of borrowers or companies seeking funds, and their level of assistance or otherwise in case of loss, such as where borrowers default in peer-to-peer lending arrangements. Continued surveys of platform practices from 2014 then fed into the FCA's further development of crowdfunding regulation in 2019,[41] where more precise regulation of platforms' conduct was introduced.[42] The EU's regulation which was introduced in 2020 also benefited from a relatively long period of gestation and culminated in certain precise conduct regulations for platforms, fund-raisers and fund-providers.[43] This allowed small business issuers to be subject to minimum cost to enter the fund-raising market, but ensured that platforms, which dealt directly with investors, bore the greater burdens of clear communication, investor protection and responsible conduct. Investors were also expected to engage in self-care in ensuring that they had adequate levels of knowledge to participate in these markets.

---

[39] EC, *Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937*, [2020] OJ, L 347/1 [EU Crowdfunding 2020].

[40] Cary Coglianese & Evan Mendelson, "Meta-Regulation and Self-Regulation" in Robert Baldwin, Martin Cave, & Martine Lodge, eds., *The Oxford Handbook of Regulation* (Oxford: Oxford University Press, 2010) at 146-168; Christine Parker, *The Open Corporation* (Cambridge: Cambridge University Press, 2002); Christine Parker, "Meta-Regulation: Legal Accountability for Corporate Social Responsibility" in Doreen McBarnet, Aurora Voiculescu & Tom Campbell, eds., *The New Corporate Accountability: Corporate Social Responsibility and the Law* (Cambridge: Cambridge University Press, 2009), online: *Social Science Research Network* <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=942157>; Colin Scott, "Regulating Everything: From Mega- To Meta-Regulation" (2012) 60:1 Administration 61.

[41] Such as the failure of peer-to-peer (p2p) lending platforms Lendy, House Crowd, etc.; see Jeremy Goldring "UK: When Peer-to-peer Lenders Fail, Who Takes The Hit?" (23 February 2022), online: *Mondaq* <https://www.mondaq.com/uk/insolvencybankruptcy/1154438/when-peer-to-peer-lenders-fail-who-takes-the-hit>.

[42] Further discussion below.

[43] Eugenia Macchiavello, "What to Expect When You Are Expecting a European Crowdfunding Regulation: The Current 'Bermuda Triangle' and Future Scenarios for Marketplace Lending and Investing in Europe" (2019) European Banking Institute Working Paper No. 55, online: *Social Science Research Network* <https://ssrn.com/abstract=3493688>; *ibid*.

The UK and EU's crowdfunding regulations task platforms with the bulk of conduct regulations, therefore allowing more proportionate obligations to be imposed on fund-raisers such as borrowers and small businesses raising equity. Unlike the US regime which continues to impose on crowdfunding issuers mandatory disclosure to investors,[44] the UK refrains from standardising issuer mandatory disclosure, obliging platforms instead to make disclosures of relevant investment information and their relevant policies.[45] The EU requires platforms to provide a standardised "key information" disclosure document. Although fund-raisers would be expected to contribute to this, they are not directly imposed with the obligation.[46] Further, investor protection is a more "dispersed" concept as regulation imposes obligations on investors to show eligibility to invest, instead of shifting the entire protective burden onto fund-raisers (as is under the traditional securities regulation model). The FCA requires investors to take appropriateness tests and to be subject to a mandatory 24-hour cooling-off period for first-time investors,[47] while the EU subjects investors to entry tests and provides a pre-contractual reflection period of four days.[48] The FCA continues to impose a cap on investible assets on crowdfunding platforms for retail users while the EU integrates a maximum loss amount into its entry test, with such amount resembling the FCA's cap.[49]

The institution of *lex specialis* allows financial regulators to meet their pro-competition objectives and to address the balances needed in their regulatory objectives explicitly. The *lex generalis* of the EU's *Digital Services Act* (DSA) for platforms discussed below would, for example, not be able to address financial regulators' specific needs.

The *lex specialis* for crowdfunding platforms and the *lex generalis* in the EU DSA similarly recognise that platforms need to assume certain responsibilities in their role of providing multisided markets and intermediating information relating to users.[50] However, the *lex generalis* is concerned more broadly with a range of personal or reputational harms that entail from illegal or hazardous content, and not specific financial harm to investors in the manner that financial regulators are concerned about. Further, the generalist governance of platforms also relies more on ex post enforcement and remedial powers for regulators than precise ex ante obligations for financial platforms, which involve prudential and risk management concerns.

The EU DSA refers to "online harms" and illegal content, and regulators are able to exercise powers to order investigation and removal of content. Platforms do not have a proactive duty to monitor content all the time and this is a different stance from the proactive duties that financial regulators are able to impose on crowdfunding platforms for specific investor protection objectives.[51] Online crowdfunding platforms in the UK are subject to specific ex

[44] Yanzhe Li, "The Regulation of Equity Crowdfunding in the US: Remaining Concerns and Lessons from the UK" (2022) 22 J. Corporate L. Studies 265.
[45] FCA Handbook, *supra* note 38 (see COBS 4.7.1).
[46] EU Crowdfunding 2020, *supra* note 39, arts. 23, 24.
[47] FCA Handbook, *supra* note 38 (see COBS 4.7.7., 4.12A.18).
[48] EU Crowdfunding 2020, *supra* note 39, arts. 21, 22.
[49] *Ibid*., art. 21.
[50] EU DSA, *supra* note 11 (the UK counterpart is the Online Safety Bill first read in Parliament at end 2022).
[51] *Ibid*., arts. 7-9, 21.

ante financial promotions regulation, in order to ensure that only certain investors can be shown crowdfunding opportunities, and mandatory warnings and content must be provided.[52] Further, *lex generalis* imposes precise internal governance requirements such as risk assessment and mitigation only for very large platforms that may engage with systemic risk.[53] However, financial regulators impose on all regulated crowdfunding platforms certain precise governance expectations, such as: prudential risk management moderated by levels of own fund requirements and business continuity policies,[54] including borrower default recovery policies for peer-to-peer lending platforms.[55]

In sum, this part has argued that enabling objectives to promote innovation and competition are strongly reflected in financial regulators' institution of *lex specialis* and their precise governance designs. Such enabling objectives are not necessarily part of *lex generalis*. Although *lex generalis* addresses the same technological phenomenon, its approach may also be insufficient for financial sector regulatory objectives in terms of prudence and conduct.

This part ends with a brief observation as to why many jurisdictions have been slow to enact *lex specialis* for crypto-finance. Consistent with the argument made here, many jurisdictions' choice to refrain from introducing a *lex specialis* for crypto-assets or crypto-finance likely reflects the lack of an enabling motivation for regulators. It is less clear that cryptocurrency is financially inclusive in nature, as the need to safekeep one's cryptocurrency, which is a digital data string, in a wallet application (that may not be safe from cybersecurity risks), is not exactly user-friendly for many. Crypto-assets however provide pre-development fund-raising for code developers and is a further decentralised form of crowdfunding from online crowdfunding discussed above.[56] In this manner, the EU has bought into the persuasion that an enabling regime is needed for crypto-assets that promise a bundle of utility and other rights upon development,[57] and has taken leadership in designing proportionate issuer obligations. The US and UK are catching up with legislative consultations and progress.[58] However, all jurisdictions take a relatively narrow approach to the enabling needs of crypto-finance, as other types of crypto-finance such as asset-backed stablecoins are subject to much more restrictive rules of governance.[59] Regulators remain

---

[52] FCA Handbook, *supra* note 38 (see COBS 4.7.6C- 6O).
[53] EU DSA, *supra* note 11, arts. 33-35.
[54] FCA Handbook, *supra* note 38 (see IPRU-INV 12.2.4, COBS 18.12.28, 33-38).
[55] *Ibid.* (see COBS 18.12.5-17, 23-27); on platforms' governance responsibilities and risk management, see *ibid.* (see COBS 18.12.18-23).
[56] Chiu, "Regulating", *supra* note 19 (see chapter 5).
[57] The Markets in Crypto-assets Regulation 2023; compromise text between the EU Council and Parliament dated October 2022 can be found at EC, *Letter to the Chair of the European Parliament Committee on Economic and Monetary Affairs*, [2022] OJ, COD 2020/0265, online (pdf): *European Commission* <https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf>; I argue for an enabling regime for crypto-assets based on the innovations of peer-to-peer business development, see *ibid*. (see chapter 2).
[58] The proposed Lummis-Gillibrand "Responsible Financial Innovation Act," which is likely not to be considered in Congress until 2023; see also HM Treasury, "Future Financial Services Regulatory Regime for Crypto-assets" (1 February 2023), online: *UK Government* <https://www.gov.uk/government/consultations/future-financial-services-regulatory-regime-for-cryptoassets>.
[59] EU DSA, *supra* note 11; Notes 65-67 above. The Lummis-Gillibrand Act proposes to limit the issuance of fiat-backed stablecoins to regulated banks, which is not dissimilar to the position taken in the EU MiCAR. The UK's

cautious of financial assets purportedly developed outside of the supremacy of fiat-denominated currency, even if many wealth managers consider them a part of portfolio diversification that mitigates correlations.[60] Many aspects in crypto-finance, such as DeFi,[61] also present many potentially anti-establishment disruptions that have yet to convince regulators in terms of their competitive, inclusive or pro-innovation benefits. The slowness in policy development for crypto-finance in many jurisdictions can be attributed to the complexities of crypto-finance in relation to different features and purposes, as well as multiple regulatory objectives that interact in relation to governing them. This makes it uncertain if *lex specialis* would be developed for crypto-finance and to what extent.

(b) The Financial Stability Objective

We next turn to an example of *lex specialis* in financial regulation that carves out a regime for regulatory oversight, albeit in a line of business that is very much cross-sectoral in nature. Such *lex specialis* allows financial regulators to govern information and communications technology (ICT) risks and third-party providers of digital infrastructure to financial institutions.[62] Such *lex specialis* is pursuant to financial regulators' perception that *lex generalis* for these technological developments would unlikely adequately cater for financial regulatory objectives, such as the protection of business continuity and financial stability. However, this part shows how such *lex specialis* cannot be a closed or exclusive regime and continues to interact with *lex generalis*, as both financial and non-financial businesses are exposed to similar issues and risks.

Financial business models have increasingly digitalised their back offices and incorporated digital and online interfaces, with this trend ramping up from the age of fintechs and the explosion of remote servicing needs during the COVID-19 pandemic.[63] This trend is not unique to financial businesses, as the digitalisation of business models and structures is taking place in a cross-sectoral manner. Further, business digitalisation often involves third-party suppliers for ICT services to a larger or smaller extent. Cloud computing infrastructure providers, for example, can provide modular ICT services to businesses from whole

---

proposals for fiat-backed stablecoins would be brought in line with payment services regulation, under the Financial Services and Markets Bill 2022, while other crypto-intermediation, custodial, lending and trading activities are proposed to be subject to regulatory principles not dissimilar to functionally equivalent incumbents' regulatory regimes.

[60] See e.g. The Economist, "Why it is wise to add bitcoin to an investment portfolio" (25 September 2021), online: *The Economist* <https://www.economist.com/finance-and-economics/2021/09/25/why-it-is-wise-to-add-bitcoin-to-an-investment-portfolio>.

[61] See Fabian Schär, "Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets" (2021) 103:2 Federal Reserve Bank St. Louis Rev. 153, online: <https://files.stlouisfed.org/files/htdocs/publications/review/2021/04/15/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets.pdf>; Jonathan Chiu, Charles M. Kahn & Thorsten V. Koeppl, "Grasping Decentralized Finance Through the Lens of Economic Theory" (2022) 55 Can. J. Economics 1702 on potential efficiency improvements with DeFi.

[62] See e.g. EC, *Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*, [2022] OJ, L 333/1, online (pdf): *European Commission* <https://data.consilium.europa.eu/doc/document/PE-41-2022-INIT/en/pdf> [EU DORA].

[63] FSB, "FinTech and Market Structure in the COVID-19 Pandemic: Implications for Financial Stability" (21 March 2022), online: *FSB* <https://www.fsb.org/2022/03/fintech-and-market-structure-in-the-covid-19-pandemic-implications-for-financial-stability/>.

infrastructures at the front, operational or back ends, to data storage and backup, suites of applications and server capacity etc.[64] In this landscape, major cloud infrastructure providers such as Amazon Web Services and Microsoft Office have become dominant players.[65]

The importance and extensiveness of digitalisation in the financial sector raises new forms of operational risks.[66] At the firm level, ICT errors and outages may cause firms and their customers, counterparties and stakeholders to suffer inconvenience and firms to suffer financial losses. Further, external threats and attacks in relation to cybersecurity breaches or incidents can cause inconveniences and losses that range from being mild to severe. A particular type of cybersecurity breach, which is the unauthorised leak of data held in financial institutions, such as customers' financial details, can result further in risks of reputational loss for the financial institution concerned, personal risks for customers and increased risks of fraud and crime in the financial system. Firms' ICT risks are not only generated from internal structures but can arise at the end of their third-party service providers if these should suffer from errors, outages or attacks.[67] Lehr argues that ICT outsourcing creates a need for the outsourcer to be able to provide "hyper-reliability" in relation to the accuracy, speed and effectiveness of the third-party's services, hence creating greater risks of such expectations not being met and entailing consequences for firms and their users and stakeholders.[68] Further, there are concerns that financial firms' ICT risks can result in systemic impacts, such as where networks are interconnected and disruption to markets for financial transactions can speedily affect many participants.[69] Where a firm's ICT risk materialisation causes a knock-on effect on other firms connected by way of transaction, collateral, credit or other economic relationships, a firm's ICT operational risk can become a source of contagious financial risk to other parties.

---

[64] Blanchette, *supra* note 10; Maziar Peihani "Financial Regulation and Disruptive Technologies: The Case of Cloud Computing in Singapore" (2017) Singapore J. Leg. Studies 77; the survey of cloud migration by European banks in 2016 is relatively cautious, see W. Kuan Hon & Christopher Millard, "Use by Banks of Cloud Computing: An Empirical Study" (2016) Queen Mary University of London, School of Law Legal Studies Research Paper No. 245/2016, online: *Social Science Research Network* <https://ssrn.com/abstract=2856431>; but uptake is expected to increase, see Colleen Baker, David Fratto & Lee Reiners, "Banking on the Cloud" (2020) 21 Transactions: Tenn. J. Bus. L. 381, online*: Social Science Research Network* <https://ssrn.com/abstract=3647392>.

[65] Sergio Gorjón, "BigTechs and Financial Services: Some Challenges, Benefits and Regulatory Responses" (2021) Banco de Espana Working Paper No. 39/21, online: *Social Science Research Network* <https://ssrn.com/abstract=3960692>.

[66] Iñaki Aldasoro et al., "Operational and Cyber Risks In the Financial Sector" (2020) Bank for International Settlements (BIS) Working Paper No. 840, online: *BIS* <https://www.bis.org/publ/work840.pdf>.

[67] Majory S. Blumenthal, "Finding Security in the Clouds" in Christopher S. Yoo & Jean-François Blanchette, eds., *Regulating the Cloud* (Cambridge, Massachusetts: MIT Press, 2015) (see chapter 2 on security risks in cloud infrastructure); Jonathan Cave et al., "Understanding Regulatory and Consumer Interest in the Cloud" in Christopher S. Yoo and Jean-François Blanchette, eds., *Regulating the Cloud* (Cambridge, Massachusetts: MMIT Press, 2015) (see chapter 6 on a range of other consumer and legal risks).

[68] William Lehr, "Reliability and Internet Cloud" in Christopher S. Yoo and Jean-François Blanchette, eds., *Regulating the Cloud* (Cambridge, Massachusetts: MIT Press, 2015) (see chapter 3).

[69] Tom C.W. Lin, "Compliance, Technology and Modern Finance" (2016) 11 Brooklyn J. Corporate Financial & Commercial L. 159 (describes these systemic impacts as "too fast to save" or "too interconnected to fail").

In the EU, the newly introduced *Digital Operational Resilience Act* (DORA) deals comprehensively with all regulated financial institutions' ICT risks.[70] Such regulation creates *lex specialis* for governing financial institutions' management of ICT risks although similar ICT risks are also faced by businesses in other sectors. The *lex specialis* carves out for financial institutions a more precise governance space from the hitherto applicable *lex generalis*, under the EU NIS Directive regime.[71] Although the EU NIS Directive has now been upgraded and amended for member states to bring into force by 18 October 2024,[72] the DORA would still cater for specific financial sector concerns in relation to ICT risks and third-party outsourcing of ICT services.

Prior to the DORA, the European Banking Authority had already recognised that ICT and cyber risks pose hazards to payment providers' and banks' business continuity and resilience, and issued guidelines for treating this area of operational risk as in particular need of ex ante governance.[73] The European Banking Authority (EBA) drew from the qualitative regulation of corporate governance and internal control for banks to extend management-based regulation to ICT risk management,[74] calling for dedicated personnel to oversee ICT systems, the formulation of policies, monitoring, testing and reporting. The DORA has drawn from and hardened many of the EBA guidelines, but has gone beyond management-based regulation to create a specific regulatory regime for ex ante management of ICT risks, in order to govern such risk management by prevention instead of remediation.

The DORA has expressly been acknowledged to impose higher and more precise requirements than under *lex generalis* that deals with cybersecurity governance in business.[75] The EU's NIS Directive 2016 introduced a minimum harmonised approach for member states to institute state-level oversight of cybersecurity threats and response

---

[70] EU DORA, *supra* note 62.

[71] EC, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, [2016] OJ, L 194/1 [NIS Directive].

[72] EC, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148*, [2022] OJ, L 333/80 [NIS 2 Directive].

[73] European Banking Authority (EBA), "EBA Guidelines on ICT and Security Risk Management" (29 November 2019), online (pdf): *EBA* <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/december/guidelines-on-ict-and-security-risk-management.pdf>; which remains adopted by the Bank of England after Brexit, as specified in Bank of England & Prudential Regulation Authority (PRA), "Interpretation of EU Guidelines and Recommendations: Bank of England and PRA approach after the UK's withdrawal from the EU" (last modified 29 November 2022), online (pdf): *Bank of England* <https://www.bankofengland.co.uk/-/media/boe/files/paper/2021/interpretation-of-eu-guidelines-and-recommendations-boe-and-pra-approach-sop-november-2022.pdf?la=en&hash=1AD2F2EEFCD4A1349F090320A23900345103541C>.

[74] EBA, "Final Report on Guidelines on internal governance under Directive 2013/36/EU" (2 July 2021), online (pdf); *EBA* <https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/1016721/Final%20report%20on%20Guidelines%20on%20internal%20governance%20under%20CRD.pdf> [EBA Guidelines]; For a conceptualisation of the prudential regulation of firms' internal organisational and governance structures for prudential regulatory objectives, see Iris H-Y Chiu, *Regulating (from) the Inside: The Legal Framework for Internal Control in Banks and Financial Institutions* (Oxford: Hart, 2015).

[75] EU DORA, *supra* note 62 (see preamble 16).

structures. These however focus on "essential services providers" as the regulatory objective is centred more broadly on national security and prevention of major social disruption.[76] Essential service providers remain the focus under the amended NIS 2 Directive, but improvements have been made from the former meta-regulatory approach. Under the first NIS Directive, firms are asked to put in place systems for business security, incident handling, business continuity management, monitoring and testing, but no prescriptive standards are specified.[77] The NIS 2 Directive has now introduced more governance and controls in terms of Board, senior management and internal control oversight of ICT systems and risks, as well as a suite of best practices conformant with specified industry certification standards, such as pertaining to incident handling, ensuring business continuity and supply chain resilience, as well as cyber-hygiene and cyber-training for staff.[78] The general standards for cybersecurity management continue to be developed by both the ICT provider industry,[79] which focuses on technical management, as well as insurance providers who have placed demands on their corporate clients to manage ICT and cyber risks in ways that mitigate insurers' financial risks.[80] The NIS regime also continues to focus on major incident reporting and a coordinated national approach to incident response as a national security concern. This objective, as Buckley et al argue, is a different objective from sector-specific regulatory objectives.[81]

Lex generalis that is cross-sectoral in nature may suffer from the disadvantage of not being able to offer more precise forms of governance for sectoral objectives. The DORA is able to target specific implications of technology risks for regulatory objectives,[82] i.e. relating to preserving business continuity, the stability of financial systems and the prevention of financial crime. In this manner, it may be warranted for financial regulators to govern ICT risks *as such* and also extend their oversight to non-financial businesses that are "critical infrastructure third-party providers."

The UK's incoming Financial Services and Markets Bill has also turned its attention to critical third-party service providers to financial institutions, but its coverage of ICT risk governance requires further detail.[83] In the absence of the DORA applying to the UK, the UK's default position on financial institutions' ICT risks is based on the EBA's guidelines mentioned above, which, although serving as the template for DORA, is more meta-regulatory in

---

[76] NIS Directive, *supra* note 71, art. 6 (see transposition in the UK *NIS Regulations 2018*, Reg. 12 for example).
[77] *Ibid.*, arts. 14, 16.
[78] NIS 2 Directive, *supra* note 72, arts. 20, 21, 24, 25.
[79] Benjamin Blakely, Jim Kurtenbach & Lovila Nowak, "Exploring the Information Content of Cyber Breach Reports and the Relationship to Internal Controls" (2022) 46 Intl. J. Accounting Information Systems 100568; Heather Buker, "Financial Institutions Adapting to Cybersecurity Modification Regulations" (2021) Capella University PhD Thesis, online (pdf): *Proquest* <https://media.proquest.com/media/hms/PFT/2/VRGiK?_s=3y8KHrJTD%2Fwmd06VrCt1hlvoMhc%3D> concludes that ICT and cyber risk management is not fully integrated into business or enterprise-wide risk management in many organisations. Although much of the data gathered in these reports are US-based, the US has a similar regime for national cybersecurity strategy and incident reporting similar to the NIS Directive.
[80] Trey Herr, "Cyber Insurance and Private Governance: The Enforcement Power of Markets" (2021) 15 Regulation & Governance 98.
[81] Ross P. Buckley et al., "Techrisk" (2020) Singapore J. Leg. Studies 35.
[82] Also earlier argued in Anton Didenko, "Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and beyond" (2020) 25 Uniform L. Rev. 125.
[83] *Financial Services and Markets Bill* [HL] (UK), 2022-2023 sess., Bill 124 (see clauses 18, 19).

nature. The EBA Guidelines principally focus on management, governance, systems, control, oversight and reporting on the part of the financial institution.[84] One empirical study has highlighted the limitations of management-based governance of ICT risks,[85] meaning that the prescription of certain best practices could more effectively address such limitations. The DORA goes beyond designating management-based governance. As a baseline, financial institutions still have to put in place senior management strategy and oversight, as well as systems for internal and risk control, and recording of all ICT-related incidents and cyber threats.[86] However, the DORA specifically requires the adoption of particular practices including: preventive practices such as strong authentication for access to data; the need for detection of anomalous activities; response and recovery; the institution of back-up systems; procedures for communication to regulators and stakeholders; the need for systems to be regularly updated and the carrying out of 3-yearly mandatory "threat-led penetration testing" by firms to test their resilience to cybersecurity attacks.[87] The UK relies on supervisory oversight such as in relation to regulators' stress-testing (which must expressly incorporate ICT risks),[88] but EU member state regulators would be able to engage with supervisory monitoring in terms of ex ante compliance as well as stress-testing.

Financial regulators recognise that critical third-party provider failures can cause potentially severe impact on financial institutions' business continuity and stability, entailing systemic impact as well. Hence, both the EU and UK have taken the novel step of extending financial regulators' remit to "critical third-party providers" which are essentially non-financial businesses. This approach deviates from the usual approach of delegating to financial firms the responsibilities for monitoring and managing their outsourcing arrangements.[89] The DORA provides more prescriptively that firms should engage in pre-contractual diligence of potential third-party providers, including considerations regarding concentration of services provided by such third-party providers to the firm.[90] Further, firms must ensure contractual adoption of certain important terms that pertain to risk management, data protection,

---

[84] EBA Guidelines, *supra* note 74.

[85] Jamelia M. Andersen-Princen, "Cloud Outsourcing in the Financial Sector: An Assessment of Internal Governance Strategies on a Cloud Transaction Between a Bank and a Leading Cloud Service Provider" (2022) 23 European Bus. Organisations L. Rev. 905.

[86] EU DORA, *supra* note 62, arts. 5-8, 17-21.

[87] *Ibid*., arts. 9-14, 26-27; there is for example no federal law in the US imposing DORA-type obligations on regulated financial services providers, but state-based legislation such as in New York can exceed the limits of federal law, see Jeff Kosseff, "New York's Financial Cybersecurity Regulation: Tough, Fair and National Model" (2017) 1 Geo. Technology L. Rev. 436; Rebecca Rabinowitz, "From Securities to Cybersecurity: The SEC Zeroes In on Cybersecurity" (2020) 61 Boston College L. Rev. 1535.

[88] PRA, "Statement on the 2022 Cyber Stress Test: Retail Payment System" (13 December 2021), online: *Bank of England* <https://www.bankofengland.co.uk/prudential-regulation/publication/2021/december/cyber-stress-test-2022-retail-payment-system>; note however that the ICT or cyber risk only featured significantly in the stress-testing for payment system providers (which is voluntary) and the mandatory Bank of England stress testing for banks in 2022 did not explicitly incorporate ICT or cyber risk; see Bank of England, "Stress testing the UK Banking System: Key Elements of the 2022 Annual Cyclical Scenario" (last accessed 9 June 2022), online: *Bank of England* <https://www.bankofengland.co.uk/stress-testing/2022/key-elements-of-the-2022-stress-test>.

[89] EBA, "Final Report on Guidelines on Outsourcing Arrangements" (25 February 2019), online (pdf): *EBA* <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1>.

[90] This regulatory design is discussed in Peihani, *supra* note 64.

access and recovery, cooperation with supervisory authorities and exit rights that do not affect the financial institution's business continuity.[91] Firms are also asked to consider adopting standardised terms developed by public sector bodies in such procurement arrangements.[92] Further, every designated critical third-party provider, whether located in the EU or otherwise, would be subject to an EU-level lead supervisor which would be one of the three pan-European financial regulatory agencies amongst the European Banking Authority, European Securities and Markets Authority or European Insurance and Occupational Pensions Authority.[93] The UK envisages that the FCA should also have direct oversight of third party critical infrastructure providers, but details remain to be fleshed out.

Has *lex specialis* for financial institutions' ICT risks and the extension of financial regulators' oversight of non-financial business suppliers eclipsed any relevance of *lex generalis* in this area? It may be too simplistic to see this area of governance as attaining a uniquely distinct "financial" character that removes from the need to interact with *lex generalis*. Financial regulators' direct oversight of critical third-party service providers brings them into interactions with non-financial businesses. Regulators should perhaps avoid a "financially-siloed" form of supervisory oversight that ignores other aspects of these non-financial businesses. This is because a holistic perspective may give regulators more informed insight as to whether and how these entities may be vulnerable to ICT risks themselves. Further, there is express acknowledgement that the DORA as *lex specialis* should continue to provide lessons for *lex generalis*.[94] Non-financial businesses in other sectors also rely extensively on ICT infrastructures and those supplied by third-party providers, and it cannot be said that other sectors would not suffer similar problems regarding business continuity and other forms of economic and social disruptions that are not less severe than threats to financial stability. Hence, the DORA expressly stipulates that there should continue to be cross-sectoral learning between the financial and business sectors in relation to cybersecurity governance, compelling financial regulators to work with other cybersecurity regulators. In this manner, although the DORA specifically carves out *lex specialis* for financial regulators' oversight, it contains reservations admitting the need to interact with *lex generalis*. Further, the DORA's sector-specific prescriptions may offer lessons for the development of *lex generalis* in due course. The next section turns to the importance of *lex generalis* for financial regulators and implications for regulatory designs and structures.

3. THE IMPORTANCE OF *LEX GENERALIS*

Lex generalis offers "across-the board" technological governance in two important respects. First, *lex generalis* is able to map out a more comprehensive set of regulatory goals for technological governance, of which financial regulatory goals are a subset. In this manner financial regulatory objectives can interact and interrelate with other "non-financial" regulatory objectives. Second, *lex generalis* fosters an "inter-disciplinary" perspective in technological governance and this contributes to a richer, more informed and more resourced governance landscape.

---

[91] EU DORA, *supra* note 62, arts. 28-30.
[92] *Ibid.*, art. 30(4).
[93] *Ibid*., arts. 31-35.
[94] *Ibid*., art 49 (see also preamble 18).

Where technological transformation is powered by data processing revolutions, we observe the dominance of *lex generalis* in technological governance. The development of big data processing, now feeding into machine learning, has pervaded many business sectors including finance. Data governance is a development in *lex generalis* and the EU is also proposing a regulation of artificial intelligence systems as a cross-sectoral measure.[95] Although there are many specific machine learning applications in finance, the governance landscape is dominated by *lex generalis*.

The use of artificial intelligence systems (AI) in finance, particularly machine learning methodologies to automate data-intensive tasks or make predictive decisions, has proliferated. In terms of data-intensive tasks, financial institutions are increasingly purchasing machine learning AI systems to deal with data processing, screening and detection of potential money laundering or scams,[96] as well as to deal with increased burdens in regulatory reporting and returns.[97] In terms of automation that benefits from speed, financial institutions have been automating trading decisions programmed to take place within various market parameters. Hyper-speed automated trading has become a trading strategy for high frequency trading firms that extensively use algorithmically programmed trading systems.[98]

Further, financial institutions are also increasingly using machine learning AI systems to make predictive decisions.[99] One area of significant development is in algorithmic credit scoring that assists financial institutions to make lending decisions. These systems are able to process more data and non-traditional forms of data regarding borrowers, such as data aggregated from platform and social media activities. These developments promote financial inclusion, but there are also certain exclusionary effects. For borrowers with less conventional conditions and who face difficulties with traditional venues of credit,[100] such as having no permanent place of abode, algorithmic credit scoring systems are able to transcend certain human judgmental biases and evaluate data more objectively and consistently regarding the data subject. However, these algorithmic credit scoring systems have at the same time also been criticised to be exclusionary or discriminatory against certain categories of borrowers based on biased historical information that the systems

[95] Discussed below.

[96] Larry D. Wall, "Some Financial Regulatory Implications of Artificial Intelligence" (2018) 100 J. Bus. & Economics 55.

[97] Iris H-Y Chiu, "Transparency Regulation in Financial Markets- Moving into the Surveillance Age?" (2011) 3 European J. Risk & Regulation 303; Philip Treleaven, "Financial Regulation of Fintech" (2017) 3:3 J. Financial Perspectives 1.

[98] Many commentators argue that the speed or frequency of trading enabled by technology is not per se an issue and abusive practices that are deceptive and manipulative should be enforced against regardless of automation or speed, see Ricky Cooper, Michael Davis & Ben Van Vliet, "The Mysterious Ethics of High Frequency Trading" (2016) 26 Bus. Ethics Q. 1; Imad Moosa, "The Regulation of High Frequency Trading: A Pragmatic View" (2015) 16 J. Banking Regulation 72.

[99] Ross P. Buckley et al., "Regulating Artificial Intelligence in Finance: Putting the Human in the Loop" (2021) 43 Sydney L. Rev. 43.

[100] Holli Sargeant, "Algorithmic Decision-Making in Financial Services: Economic and Normative Outcomes In Consumer Credit" (21 November 2022), online: *Springer* <https://doi.org/10.1007/s43681-022-00236-7>.

have been trained with.[101] These subconscious social biases imbued in training data are learnt by AI systems and replicate into exclusionary or discriminatory credit decisions. Another area where predictive decisions may increasingly be placed into the hands of machine learning AI systems is that of investment management. The Evovest fund, for example, is managed entirely by algorithmic programming based on comprehensive data carefully labelled regarding asset, market, sectoral, jurisdiction and wider geopolitical developments.[102]

The adoption of AI systems in finance entails risks that affect financial regulatory objectives, as well as wider social concerns beyond financial regulatory goals. For example, automated trading programmes have on more than one occasion caused temporary price crashes which required intervention from exchanges and financial regulators,[103] in order to maintain the stability and continued functioning of financial markets. In this respect, such AI systems pose financial stability risks, a concern squarely within financial regulators' objectives. Regulators have refrained from banning such trading due to perceived liquidity and market-making benefits.[104] However, high frequency trading also raises issues regarding fairness for participation in financial markets. Exchange co-location practices for high frequency firms' servers potentially discriminate against market participants that are less technologically-resourced.[105] It is generally questioned if high-frequency trading merely contributes to selfish accumulation in a manner that can adversely harm social good.[106] The fairness narrative has however not permeated financial regulatory perspectives which are dominated largely by economic paradigms.[107]

Next, the exclusionary and discriminatory aspects of credit, insurance or investment screening by algorithms are relevant to the financial regulatory objectives of investor and consumer protection, in terms of whether access and fair treatment are affected. Any application of automated management of customers' financial mandates may also run the risk that decisions are made which are not in the best interests of customers. These risks and regulatory objectives concern financial regulators, but are however part of a broader picture. Customer risks entail from the data governance of machine learning AI systems used by financial services providers. AI systems vary in terms of how data is labelled,

---

[101] Katja Langenbucher, "Responsible A.I.-based Credit Scoring – A Legal Framework" (2020) 31 European Bus. L. Rev. 527; Nikita Aggarwal, "The Norms of Algorithmic Credit Scoring" (2020) 80 Cambridge L.J. 42, online: *Social Science Research Network* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3569083>.

[102] Sylvie St-Onge, Catherine Vincent & Michel Magnan, "Artificial Intelligence in an Emerging Portfolio Manager: The Case of Evovest" in Duc Kuong Nguyen, ed., *Handbook of Banking and Finance in Emerging Markets* (Cheltenham: Edward Elgar, 2022) (see chapter 28).

[103] Chartered Financial Analyst (CFA), "Flash Crashes" (last accessed 9 June 2023), online: *CFA Institute* <https://www.cfainstitute.org/en/advocacy/issues/flash-crashes#sort=%40pubbrowsedate%20descending> (on the flash crashes that occurred in 2010 and 2015).

[104] Discussed in Andrea Roncella & Ignacio Ferrero, "The Ethics of Financial Market Making and Its Implications for High-Frequency Trading" (2022) 181 J. Bus. Ethics 139.

[105] Trude Myblebust, "Fairness and Integrity in High-Frequency Markets – A Critical Assessment of the European Regulatory Approach" (2020) 31 European Bus. L. Rev. 33.

[106] Roncella & Ferrero, *supra* note 104.

[107] See e.g. UK Financial Conduct Authority (UK FCA), "Occasional Paper No. 13: Economics for Effective Regulation" (last modified 2 September 2016), online: *UK FCA* <https://www.fca.org.uk/publications/occasional-papers/occasional-paper-no-13-economics-effective-regulation>.

processed and trained. Supervised machine learning systems rely on human determination in labelling data and outcomes, while unsupervised systems need large quantities of representative data for training and testing. In this manner, consumer or investor protection risks are not merely a matter for financial intermediaries' "conduct" and relationship with customers, but are closely related to the broader issues of data governance in machine learning AI systems.[108] Data governance is a realm shaped by broader social objectives including the legitimacy of data collection, the rights of data subjects such as privacy, power over the use of data and the responsibilities for data use that accord with social expectations of ethicality and decency.[109]

The deployment of machine learning AI systems in finance raises risks that are embedded within a broader set of regulatory goals. Hence, the basic framework for data governance is in the *lex generalis* of the General Data Protection Regulation (GDPR).[110] The GDPR now comprehensively governs private and public sector conduct in relation to how data is collected and processed. It sets out data subjects' rights in relation to privacy, sensitivity of protected categories of information and provides data subjects' rights such as the right to request erasure of information previously collected.[111] The GDPR's comprehensive governance represents the social contract regarding all businesses', including financial institutions', duty to customers in relation to their information. This is also coincidental with the erosion of the traditional "bank secrecy" duty over the years due to legal interventions based on public interest and needs.[112]

Further, the EU now proposes to govern the design of machine learning AI systems in a *lex generalis*,[113] although its compatibility with the GDPR may need further work.[114] The

---

[108] Wall, *supra* note 96; Sargeant, *supra* note 100.

[109] Ethical codes developed by corporate and not-for-profit organisations proliferate in the ethical self-regulating space at the moment, see e.g. Google's Principles on AI, Google, "Our Principles" (last accessed 9 June 2023), online: *Google* <https://ai.google/principles/>; International Business Machines (IBM), AI Ethics (last accessed 16 June 2023), online: *https://www.ibm.com/artificial-intelligence/ethics*; Institute of Electrical and Electronic Engineers' (IEEE) Standards on AI, see IEEE, "The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems" (last accessed 9 June 2023), online: *IEEE Standards Association* <https://standards.ieee.org/industry-connections/ec/autonomous-systems/>; See also Future of Life Institute, "AI Principles" (11 August 2017), online: *Future of Life Institute* <https://futureoflife.org/ai-principles/>; Luciano Floridi et al., "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations" (2018) 28 Minds & Machines 689.

[110] Intersoft Consulting, "General Data Protection Regulation" (last accessed 9 June 2023), online: *Intersoft Consulting* <https://gdpr-info.eu/>.

[111] See assessment of implementation by EU Agency for Fundamental Rights, "The General Data Protection Regulation – one year on" (29 May 2019), online (pdf): *EU Agency for Fundamental Rights* <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-gdpr-one-year-on_en.pdf>.

[112] David Chaikin, "Adapting the Qualifications to the Banker's Common Law Duty of Confidentiality to Fight Transnational Crime" (2011) 33 Sydney L. Rev. 265.

[113] European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (21 April 2021), online: *European Commission* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>.

[114] Sandra Wachter, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR" (2018) 34:3 Computer L. & Security Rev. 436, online (pdf): *University of Oxford* <https://ora.ox.ac.uk/objects/uuid:e49c4ea8-fe71-48ac-9f85-13c3e0ede718/download_file?file_format=pdf&safe_filename=Wachter%2B07.02.18.pdf&type_of_work=Journal+article>.

proposed EU regulation would categorise AI systems, including automated and not just machine learning systems, according to risks. It proposes to introduce a framework for governing AI systems in different categories of risks in relation to design, manufacture, use, continued monitoring and reporting.

The *lex generalis* for regulating AI systems addresses a broad, cross-sectoral set of social concerns and needs, such as in relation to privacy and vulnerable data subjects. The EU regulation prohibits the sale or use of AI systems that use subliminal techniques, exploits vulnerabilities of disadvantaged persons such as minors or the mentally disabled, as well as systems that engage in social scoring by public authorities. Real-time biometric information processing would also be highly limited unless justified by certain public interests such as criminal detection or prevention of terrorist acts. Such general prohibitions would also ensure that financial consumers are not subject to such systems, as part of meeting broader social objectives.

The EU regulation also proposes to allow but govern "high risk AI systems," while permitting limited or minimally risky AI systems to be subject to self-regulatory ethical codes of conduct. The list of high-risk AI systems includes credit scoring systems, but many other financial applications do not seem to be explicitly included. This position creates gaps in the protection for customers of other essential financial services such as insurance and investment. Where *lex generalis* applies to algorithmic credit scoring systems, the full regulatory obligations include: life cycle risk management and monitoring obligations on the part of manufacturers and users; extensive data governance such as ensuring representativeness, appropriate labelling and bias weeding; comprehensive technical documentation provided by manufacturers which should also be checked for completeness and accuracy by distributors and importers; mandatory logging capabilities on the part of AI systems in order to make explanations and be accountable to users and ensuring there is a human in the loop for risk mitigation and protection of fundamental rights or health and safety of users.[115] Why would these obligations not be important, for example, to trading or investment management systems that have the potential to incur significant financial losses? Data governance that affects investment strategy in terms of logging, explainability and accountability are important to wealth and fund managers, as well as to their investors. Ensuring a human in the loop to oversee financial loss risk also seems imminently sensible. If automated investment management systems are, for example, not classified as high-risk in *lex generalis*, reliance will have to be placed on self-regulatory codes or the development of *lex specialis*.

It may be argued that *lex specialis*, such as for high frequency trading, has been precisely developed by financial regulators. However, this is an ex post response to market failure. Learning from the flash crash episode of 2010, the EU's Markets in Financial Instruments Directive 2014 included a specific provision for algorithmic trading firms to put in place governance and control mechanisms and to make regular specific reporting to regulators.[116] High frequency traders that habitually trade in significant volumes are also obliged to

[115] Buckley et al., *supra* note 99.
[116] EC, *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*, [2014] OJ, L 173/349, art. 17.

maintain their market-making capacity in order to preserve financial stability during stressed times. In relation to the EU's proposal, there is a case to be made for including a wider range of consumer financial interfaces in the *lex generalis* that provides ex ante governance of AI systems. *Lex generalis*, such as relating to data governance, is able to offer consistent protections for citizenry in relation to similar risks subject to technological governance. Financial regulators would not need to duplicate those levels of protection in *lex specialis*, although specific financial regulatory issues can be explicitly addressed.

The UK also takes the approach of *lex generalis* for the governance of AI systems in a cross-sector manner.[117] However, the Conservative government, whose preference is to shy away from explicit regulation, has proposed a set of high-level cross-cutting principles for all regulators to apply in their specific contexts of use by industry. These principles relate to safety, fairness, accountability, transparency and challenge/redress for outcomes. The UK's approach shows similar policy thinking in acknowledging that certain technologies raise cross-cutting issues and a broad set of regulatory goals. The approach nevertheless allows for sectoral distinctions in governance where applying the principles is concerned. This principles-based "soft law" approach therefore articulates common governance objectives in *lex generalis* while allowing *lex specialis* to develop particular guidelines or regulation. The approach also envisages centralised government coordination for sharing of regulatory insights and continued development of policy.

Some commentators have argued for financial regulation to be transformed into more technologically responsive data-based regulation,[118] rather than seeing such governance as housed under *lex generalis*. This article takes a different view and argues that the necessary interrelationship between *lex generalis* and *lex specialis* should be acknowledged. Financial regulators should work alongside other policy-makers in the development of *lex generalis* in order to support the broader set of regulatory goals while being mindful of the need to provide for particular financial regulatory objectives that do not find their way into *lex generalis*. For example, there may be a need for special safeguards in responsible lending for algorithmic lenders as predatory lending could be a problem, rather than a lack of inclusion.[119] There may also be a need for specific forms of data governance in relation to predicting financial risks,[120] such as credit, market and operational risks, in relation to conservative interpretations of data or synthetic data for prudential management purposes.

This article takes the view that there is an inevitable interrelationship between *lex generalis* and *lex specialis* for technological transformations in finance that implicates both financial other social and regulatory objectives. The dividing line is not always clear between *lex generalis* that addresses broader social objectives such as data governance and *lex specialis* whose regulatory objectives are more distinct. Hence, it is proposed that the regulatory design and arrangements for technological governance in finance should be "inter-

---

[117] Rt. Hon. Michelle Donelan M.P. (Secretary of State for Science, Innovation and Technology), "A Pro-innovation Approach to AI Regulation" (29 March 2023), online: *UK Government* <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper>.

[118] Dirk A. Zetzsche et al., "The Evolution and Future of Data-driven Finance in the EU" (2020) 57 Common Market L. Rev. 331.

[119] Johnson, Pasquale & Chapman, *supra* note 37.

[120] Tom C.W. Lin, "Artificial Intelligence, Finance, and the Law" (2019) 88 Fordham L. Rev. 531.

disciplinary" and also "inter-agency"-based. The dominance of *lex generalis* over *lex specialis* can result in under-inclusion, in relation to sectoral developments and specific regulatory objectives. The dominance of *lex specialis* over *lex generalis* can also result in under-inclusion, as financial regulators would seek modes of governance that can be more comfortably managed within their mandates and resources, while potentially ignoring other social concerns.

In terms of the "inter-disciplinary" conduct of technological governance that involves *lex generalis* and *lex specialis*, it is proposed that sector-specific regulators work closely with regulators overseeing *lex generalis*, such as the Information Commissioner for the GDPR or the authority designated for AI systems regulation. Such inter-agency collaboration is useful at the stage of policy formation, so that agencies' concerns can be tabled more holistically while division of supervisory labour can also be forged. An example of such inter-agency learning is envisaged in the DORA which recognises that the financial regulation of critical third-party infrastructure providers does not provide a whole picture of governance, and financial regulators need to share with and learn from other relevant regulators.[121] Hence, inter-agency collaboration should also pertain to continuous learning in terms of implementation and post-implementation stages of regulatory reform. Technological governance also involves regulated firms' generation of own risk management systems and bespoke technical documentation. Sectoral and general regulators should systematically come together to share and analyse firm-level information provided to regulators so that cross-sectoral learning can be fostered. Such shared learning helps to develop best practices for firm implementation as well as risk detection and insights for supervisory conduct.

The "inter-disciplinary" conduct of regulatory governance ultimately has to be founded upon an "inter-agency" structure of cooperation and coordination. Often, formal structures for coordination and cooperation would put these on a firmer footing, as regulatory agencies can be insular for fear of exceeding their mandates. Formal structures of cooperation and coordination are also seen as necessary to respond to crises or problems, such as the computer security incident response team (CSIRT) team structure for responding to cybersecurity incidents or the coordination structures put in place between the Bank of England and Financial Conduct Authority after the 2007-9 global financial crisis.[122]

The structures proposed in the DORA regarding co-learning amongst sectoral and general regulators, as well as for emergency response, are rather vague for now, and could benefit from tightening up. Sectoral and general regulators concerned about a particular technological development should form formal forums for regular joint meetings, and further develop agendas for exploration, coordination and shared responsibilities. These fori may pave the way for the formation of quasi-formal committees or groupings for joint governance work, supervision or enforcement. Experimental sandboxes to engage with technology developers can also be inter-agency-based in order to benefit from all relevant governance insight. Further regulators engaged in inter-agency coordination and cooperation can share or jointly develop their supervisory technology (suptech) or regulatory technology (regtech) capacities in relation to employing automated or machine

[121] EU DORA, *supra* note 62, art. 49.
[122] *The Network and Information Systems Regulations 2018* (UK), SI 2018/506, s. 5, 6; *FSMA*, *supra* note 28, ss. 3D, 3E.

learning systems to manage regulatory reporting and compliance surveillance.[123] Such inter-agency liaisons have the potential to foster a stronger knowledge base for each regulator, as well as promote well-informed and considered regulatory development and crisis response in a more seamless and effective manner.

The development of "inter-disciplinary" policy thinking and inter-agency coordination should not be confined to governing AI systems.[124] Financial regulators are unlikely able to deal with all manners of technological transformations affecting finance via *lex specialis* alone. The development of *lex generalis* is important for encompassing a broader set of goals to which financial regulatory objectives relate. But *lex specialis* has a place for addressing specific needs for financial sector governance. This article argues that regulatory response benefits from being more holistic in nature, drawing on the strengths of *lex specialis* and *lex generalis*, dynamically interacting with each other, hence requiring new and joined-up ways of treating regulatory governance and fostering inter-agency coordination and learning.

We turn to the question of whether the rise of large technology companies (Bigtech) in finance should be addressed by *lex generalis* or *lex specialis*.

(a) Bigtech in Finance

Commentators have speculated as to whether Bigtech would be able to drive a coach and horses through the financial sector, radically changing the business models that have dominated direct and market-based intermediation in finance.[125] This is because Bigtechs have captured significant global market share in terms of social media membership, platform marketplace membership or other forms of network effects, giving them immense accessibility to leverage upon a vast amount of user and customer data. Such data can further be harvested, analysed and used to promote selling of financial products or engagement of financial interest, further augmenting Bigtechs' cross-sectoral market power. For example, Facebook's endeavour to develop a payment token, Libra, later renamed as Diem, alarmed regulators who feared that it may come to dominate cross-border remittance.[126]

---

[123] On using automated systems for supervisory surveillance, see Allen, *supra* note 20 (see chapter 5); Tom Butler & Leona O'Brien, "Understanding Regtech for Digital Regulatory Compliance" in Theo Lynn et al., eds., *Disrupting Finance* (London: Palgrave Studies, 2019) (see chapter 6); Ross P. Buckley et al., "The Road to RegTech: the (astonishing) example of the European Union" (2020) 21 J. Banking Regulation 26.

[124] Martin Kretschmer, Ula Furgal & Philip Schesinger, "The Emergence of Platform Regulation in the UK: An Empirical Legal Study" (last modified 16 December 2021), online: *Social Science Research Network* <https://ssrn.com/abstract=3888149> (on the need for interagency coordination for various aspects and risks of platform governance; forthcoming in Weizenbaum Journal of the Digital Society – special issue: "Democracy in Flux – Order, Dynamics and Voices in Digital Public Spheres" in 2023).

[125] Zetzsche, Buckley & Arner, "Techfins", *supra* note 37 (see chapter 13); Sylvie St-Onge, Michel Magnan & Catherine Vincent, "The Digital Revolution in Financial Services: New Business Models and Talent Challenges" in Duc Kuong Nguyen, ed., *Handbook of Banking and Finance in Emerging Markets* (Cheltenham: Edward Elgar, 2022) (see chapter 24).

[126] FSB, "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements" (13 October 2020), online: *FSB* <https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/>; Elizabeth Dwoskin & Gerrit de Vynck, "Facebook's cryptocurrency failure came after internal conflict and regulatory pushback" (28 January 2022), online: *Washington Post* <https://www.washingtonpost.com/technology/2022/01/28/facebook-cryptocurrency-diem/>.

While such consolidation of market and financial power seems to be taking place amongst a couple of Chinese Bigtechs, in particular Alibaba's subsidiary Ant Group and Tencent's Wepay service,[127] it is doubted that Bigtechs in developed financial jurisdictions in the West have made as much headway.[128] Bigtechs in the West have all forayed into diversifying payment interfaces and have picked the "low hanging fruit" in finance which does not require balance sheet operations.[129] There seems to be a slower foray into credit products, insurance or investment management.[130] It has been argued that Bigtechs' lack of dominance in finance can be attributed to the already developed financial markets in the West. Financial markets in many Western developed jurisdictions are already replete with choice in financial products. Further, incumbents enjoy the advantage of being already subject to and familiar with highly developed regulatory regimes for prudence and consumer conduct.[131] Although Bigtech dominance in UK or European financial sectors does not seem to be high on the horizon, particularly after the retreat of Facebook's Diem project,[132] regulators continue to be wary of Bigtech's potential advances and are concerned about the regulatory agenda ahead.

Where *lex specialis* applies to aspects of Bigtech's operations, such as in relation to payment services, *lex specialis* is unable to relate to the "whole picture" of Bigtechs' risks or power. In relation to *lex generalis*, the particular concern with Bigtech is whether practices are being perpetuated that entrench market power and are not sufficiently addressed by existing competition law tools. In this regard, *lex generalis* is focused on competition law, such as the EU's *Digital Markets Act*.[133] This regime governs Bigtech by classifying them as "gatekeepers,"[134] which prevent them from engaging in certain forms of conduct that augment their market power. Such conduct includes unduly locking users into bundled services or applications, preventing access by users to third-party services or applications or giving preferential treatment in marketing or promotion to the gatekeeper's own services, products or applications over others.[135] There is however a close interrelationship between Bigtechs' market power and financial regulatory objectives, such as prudential governance and financial stability. For example, Bigtechs can provide cloud infrastructure and digital services to financial institutions, while also competing with these institutions in the arenas of offering payment services and credit products. Further, Bigtechs can experiment with machine learning AI systems and deploy them in financial as well as non-financial aspects of

[127] Dirk A. Zetzsche et al., "Paradigm", *supra* note 22.
[128] Eichengreen, *supra* note 21; Frost et al., *supra* note 37.
[129] Frost et al., *supra* note 37.
[130] Amazon offers payment and credit card services, and Apple was slower to offer the Apple card. However, Google has not made similar advances other than into payment services. Further, Meta's ill-fated Diem project may serve as a warning for social media platforms in relation to forays into financial services.
[131] *Ibid*.
[132] See n126.
[133] EC, *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*, [2022] OJ, L 265/1.
[134] *Ibid.*, art. 3.
[135] *Ibid*., arts. 5-7.

their business models, hence their data and risk management needs to be scrutinised for a holistic range of risks.[136]

The potential of Bigtech in finance draws together concerns in both *lex specialis* and *lex generalis* in highly intertwined ways. There needs to be joined-up perspective regarding Bigtechs' conflicts of interest and their governance, the financial stability risks they pose in case of an outage and their overall market power.[137] In this manner, *lex specialis* for Bigtechs may entail a siloed form of financial supervision, while *lex generalis* may be too focused on competition law and may miss the interactions between financial regulatory governance and general "gatekeeper" governance for Bigtechs.

There is arguably a case for entity-based supervision for Bigtechs that is beyond supervision relating only to market competition issues.[138] One can possibly learn from the supervisory college system for financial conglomerates to ensure a coordinated form of inter-agency and inter-disciplinary supervision for Bigtechs.[139] For each Bigtech, a cross-sectoral college of relevant supervisors from major jurisdictions of the Bigtech's operations can be formed for overall oversight. In this manner, the supervisory needs for Bigtech reinforce the need for inter-agency and inter-disciplinary coordination amongst relevant regulatory agencies, elevated to an international level. It is hoped at these levels that the interactions of insights between *lex specialis* and *lex generalis* can take place, although it would be too simplistic to foreclose issues of priority contests, tradeoffs and difficult decisions where objectives conflict. Further, we do not underestimate the difficulties of regulators with different mindsets working together, such as financial regulators who focus on financial and economic indicators compared to regulators who may be focused on other needs in governance, such as social rights or justice. Such forums can however provide the first steps towards transparent and comprehensive debates regarding the relationship between *lex specialis* and *lex generalis* and the effective development of their designs. These forums should also be seen as arenas for constructive conversations and the shared forging of solutions, instead of territorial or ideological warzones.

4. CONCLUSION

Financial regulators live in dynamic times as financial, and now more than ever, technological innovations transform business models and the regulated landscape, demanding a response. As technological transformations often affect business sectors and not just finance, regulators have to grapple with the aptness of regulatory designs that are specialist and sectoral, as well as those that are more general and across-the-board. This article argues that while *lex specialis* is often warranted by precise financial regulatory

---

[136] Aline Darbellay, "Algorithm-driven Information Gatekeepers: Conflicts Of Interest in the Digital Platform Business Models" in Joseph Lee & Aline Darbellay, eds., *Data Governance in AI, Fintech and LegalTech* (Cheltenham: Edward Elgar, 2022) (see chapter 5).

[137] Gorjón, *supra* note 65.

[138] Anne C. Witt, "Platform Regulation in Europe—Per Se Rules to the Rescue?" (2022) 18 J. Competition L. & Economics 670; Lucia Pacheco, "Implementing the Principle of 'Same Activity, Same Risk, Same Regulation And Supervision': Activity Vs Entity-Based Frameworks" (last modified 15 October 2021), online: *BBVA Research* <https://www.bbvaresearch.com/en/publicaciones/global-implementing-the-principle-of-same-activity-same-risk-same-regulation/>.

[139] See the Joint Forum, "Report on Supervisory Colleges for Financial Conglomerates" (1 September 2014), online (pdf): *Bank for International Settlements* <https://www.bis.org/publ/joint36.pdf>.

objectives, there are useful consistency benefits and governance standards that can be designed at a cross-sectoral level. *Lex generalis* and *lex specialis* benefit from each other in relation to cross-sectoral learning and insights that enrich supervisory governance. Financial regulators seeking a holistic perspective affecting their own stewardship of regulatory objectives cannot ignore other needs in technological governance. Hence, financial and other regulators need to be prepared for embracing the dynamic landscape of interaction between *lex specialis* and *lex generalis*. Regulators can benefit from formalised coordinative and cooperative structures across sectors which cater for regulators' needs in knowledge-building and governance thinking. Such structures can be elevated to the international level where systemically important Bigtechs are concerned, for supervising the risks they pose to finance, economies and societies.