Cambridge Yearbook of European Legal Studies, 24 (2022), pp. 262–293
doi:10.1017/cel.2022.10

Hard Law and Soft Law Regulations of Artificial Intelligence in Investment Management

Wojtek BUCZYNSKI, CFA, FRM; PhD candidate
University of Cambridge; financial technology, regulation, and governance consultant

Felix STEFFEK
Associate Professor, Faculty of Law, University of Cambridge; J M Keynes Fellow in Financial Economics, University of Cambridge; Visiting Professor, Notre Dame Law School

Fabio CUZZOLIN
Professor of Artificial Intelligence, Visual Artificial Intelligence Laboratory, School of Engineering, Computing and Mathematics, Oxford Brookes University

Mateja JAMNIK
Professor of Artificial Intelligence, Department of Computer Science and Technology, University of Cambridge

Barbara SAHAKIAN
Professor of Clinical Neuropsychology, Department of Psychiatry, University of Cambridge and Clare Hall

Abstract

Artificial Intelligence ('AI') technologies present great opportunities for the investment management industry (as well as broader financial services). However, there are presently no regulations specifically aiming at AI in investment management. Does this mean that AI is currently unregulated? If not, which hard and soft law rules apply?

Investments are a heavily regulated industry (MIFID II, UCITS IV and V, SM&CR, GDPR etc). Most regulations are intentionally technology-neutral. These regulations are legally binding (hard law). Recent years saw the emergence of regulatory and industry publications (soft laws) focusing specifically on AI. In this Article we analyse both hard law and soft law instruments.

The contributions of this work are: first, a review of key regulations applicable to AI in investment management (and oftentimes by extension to banking as well) from multiple jurisdictions; second, a framework and an analysis of key regulatory themes for AI.

Keywords: investments, investing, financial services, AI, Artificial Intelligence, regulation, MIFID, GDPR, SM&CR, EU AI Act, cloud

I. INTRODUCTION

A. *Overview*

Artificial Intelligence ('AI') is being increasingly researched and utilised across various business areas within the investment management industry and broader financial services.[1] It can add real value through a combination of improved product and service offerings, better customer experience, better customer support, improved safety, and lower costs (both for the clients and for the investment firms).[2] At the same time, there is concern about potentially harmful (even if unintended) effects of such powerful new technologies, and the need for governance thereof.[3] Broadly speaking, three potential routes for AI governance in financial services can be identified: (1) hard law—legally binding, compulsory regulations issued by parliaments and regulators (including AI directives that require transposition into hard laws); (2) soft law—non-binding, but intended to have normative effect(s) and strongly encouraged principles issued by regulators or by influential, reputable industry groups; and (3) self-regulation by the industry, based on written or unwritten (but always non-binding) principles. This Article focuses on hard and soft laws. It excludes self-regulation as this would require a further paper. Also, following the 2008 financial crisis, deregulation and self-regulation are doubted by many.[4]

During the speech[5] inaugurating the UK AI Private-Public Forum ('AIPPF') launched jointly by the Bank of England ('BoE') and the Financial Conduct Authority ('FCA') Dave Ramsden, BoE's Deputy Governor of Markets and

---

[1] The 2021 OECD report reads: 'Artificial Intelligence (AI) techniques are being increasingly deployed in finance, in areas such as asset management, algorithmic trading, credit underwriting or blockchain-based finance, enabled by the abundance of available data and by affordable computing capacity'. OECD, 'Artificial Intelligence, Machine Learning and Big Data in Finance', 2021, https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf.

[2] The abovementioned OECD report further reads: 'The deployment of AI in finance is expected to increasingly drive competitive advantages for financial firms, by improving their efficiency through cost reduction and productivity enhancement, as well as by enhancing the quality of services and products offered to consumers'. Ibid.

[3] In the UK, the Competition and Markets Authority ('CMA') has asked for evidence on potential harm to competition and consumers caused by AI; UK Government Press Release, 'CMA Lifts the Lid on Impact of Algorithms, 19 January 2021, https://www.gov.uk/government/news/cma-lifts-the-lid-on-impact-of-algorithms. In the US, the Federal Reserve has issued a request for information ('RFI') on financial institutions' use of AI; US National Archives, Federal Register, 'Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning', 31 March, 2021, https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

[4] T J Presley and B Jones, 'Lehman Brothers: The Case Against Self-Regulation' (2014) 11(2) *Journal of Leadership, Accountability and Ethics* 11; J C Coffee Jr, 'What Went Wrong? An Initial Inquiry into the Causes of the 2008 Financial Crisis' (2009) 9(1) *Journal of Corporate Law Studies* 1.

[5] Dave Ramsden, Deputy Governor or Markets and Banking, Bank of England, Opening Remarks at the Launch of the Artificial Intelligence Public Private Forum – Speech by Dave Ramsden, 12 October 2020, https://www.bankofengland.co.uk/speech/2020/dave-ramsden-opening-remarks-for-the-launch-of-aippf.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

Banking, called the regulatory landscape around AI 'fragmented'. We concur with this assessment. One of the primary objectives of this paper is to 'defragment' and consolidate this landscape.[6]

Defining what constitutes artificial intelligence is subject to ongoing discussions among academics, regulators and policymakers. This Article takes a straightforward approach towards definitions: AI is used to describe a computer system (embodied or not) performing tasks associated with intelligence (eg reasoning, learning from past experience, discovering meaning, generalising).[7] Present-day AI is often synonymous with Machine Learning ('ML'). The terms 'AI' and 'ML' are used either jointly or interchangeably by the regulators. In this Article, the term algorithm follows a definition commonly used in computer science understanding it as a set of rules defining a sequence of operations.[8] For the avoidance of doubt: AI always utilises algorithms, but not all algorithms are AI. Many algorithms employed in financial services are purely deterministic 'if → then' solutions which fall under algorithmic regulation but are not AI.

AI is being adopted in a variety of business functions across financial services: from algorithmic trading to recruitment. This Article focuses on core functions such as investment decision making (portfolio management) and trading. Statistical data regarding the adoption of AI in investment management (particularly in core investment functions) is difficult to come by, and at times needs to be proxied through qualitative and anecdotal information. The Financial Stability Board ('FSB') report[9] is particularly candid in admitting that 'data on the extent of adoption [of AI] in various markets is quite limited'. While one can argue that the AI landscape in financial services has progressed dramatically in the five years since the publication of the FSB report in 2017, based on two, more recent, influential industry surveys—one from the Bank of England and Financial Conduct Authority ('FCA'),[10] and the other one from the CFA Institute[11]—it appears that utilisation of ML in investment decision making is currently still low. Utilisation in this context would be defined as AUM (Assets under Management—the monetary value of all the investments a given firm is managing for its clients, measured at a specific point in time)[12] exposed to ML decision making as a percentage of the overall AUM of the industry.

---

[6] The methodology of our regulatory search is detailed in Appendix 1.

[7] Encyclopedia Britannica, 'Artificial Intelligence', https://www.britannica.com/technology/artificial-intelligence.

[8] K Lum and R Chowdhury, 'What Is an "Algorithm"? It Depends Whom You Ask', *MIT Technology Review*, 26 Feb 2021.

[9] Financial Stability Board, 'Artificial Intelligence and Machine Learning in Financial Services', 2017.

[10] Bank of England and Financial Conduct Authority, 'Machine Learning in UK Financial Services', October 2019, https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf.

[11] CFA Institute, 'AI Pioneers in Investment Management', 2019, https://www.cfainstitute.org/-/media/documents/survey/AI-Pioneers-in-Investment-Management.ashx.

[12] AUM is a common top-level metric of the scale of a given investment management firm. The AUM fluctuates with the inflows and outflows of investors' money, as well as with the changes of market values of the investments themselves. Investment management industry's business model is based on

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

This Article sometimes refers to 'financial services' and to 'investment management'. The terms are not synonymous and are not to be used interchangeably. Investment management is a subset of financial services, which also include banking and insurance. While our research is focused on investment management, when applicable we make statements and inferences relevant to the financial services industry at large.

B. Research Objective

As shown in Figure 1, starting around the mid-2010s, several hard[13] and soft laws[14] have been implemented or proposed by regulators and various industry bodies worldwide. Only one hard law (the proposed EU AI Act) explicitly references AI. All the other hard laws cover it implicitly (MIFID II and RTS 6 regulate algorithms, while GDPR covers automated decision making) or tangentially (SM&CR addresses accountability, which in our view extends to management's accountability for actions and decisions made by AI).[15] Our definition of hard law includes EU directives, which require transposition by the EU Member States.

(F'note continued)
charging fees expressed as a fraction of AUM, which makes AUM one of the most important metrics in the industry.

[13] 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; European Commission, 'RTS 6', 2016; Financial Conduct Authority, 'The Senior Managers and Certification Regime: Guide for FCA Solo-Regulated Firms' ('SM&CR'), July 2019, https://www.fca.org.uk/publication/policy/guide-for-fca-solo-regulated-firms.pdf; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation), 27 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN; European Parliament, 'Proposal for an Artificial Intelligence Act', 2021; People's Bank of China, 'Guiding Opinions of the PBOC, the China Banking and Insurance Regulatory Commission, the China Securities Regulatory Commission, and the State Administration of Foreign Exchange on Regulating the Asset Management Business of Financial Institutions', 27 April 2018.

[14] European Commission, 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust', 2020; European Commission, 'Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics', 2020; European Commission, 'Liability for Artificial Intelligence and Other Emerging Digital Technologies', 2019; OECD, note 1 above; The Ministry of Economy, Trade and Industry ('METI'), 'Governance Guidelines for Implementation of AI Principles ver. 1.0', 2021; Hong Kong Monetary Authority ('HKMA'), 'High-Level Principles on Artificial Intelligence', 2019; The International Organisation of Securities Commissions ('IOSCO'), 'The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers', https://www.iosco.org/library/pubdocs/pdf/IOSCOPD658.pdf; Financial Stability Board, note 9 above; Bundesanstalt für Finanzdienstleistungsaufsicht ('BaFin'), 'Big Data Meets Artificial Intelligence – Results of the Consultation on BaFin's Report', 21 March 2019, https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2019_01/bp_19-1_Beitrag_SR3_en.html; Information Commissioner's Office, 'Guidance on the AI Auditing Framework Draft Guidance for Consultation', 2020; Information Commissioner's Office, 'Explaining Decisions Made with AI', 2020; Personal Data Protection Commission, 'Model Artificial Intelligence Governance Framework (2nd ed)', Singapore, 2020.

[15] For a complete list of hard and soft law publications please see Appendix 2.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

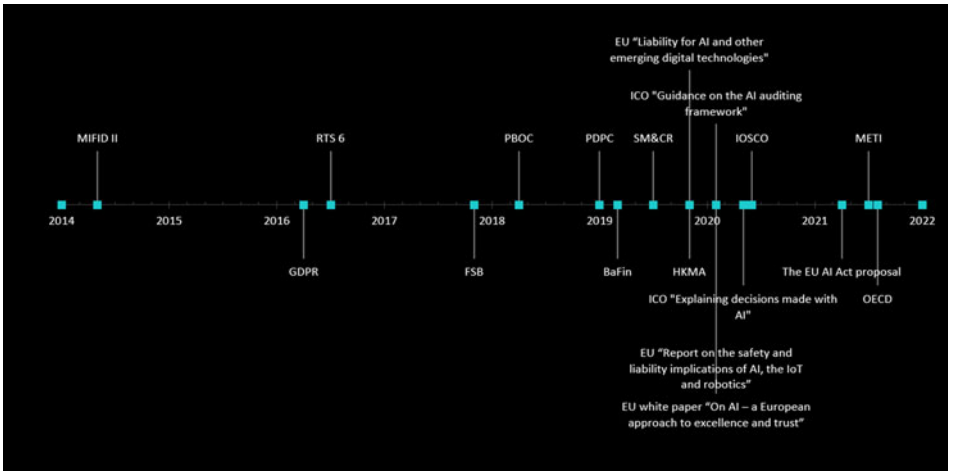

Figure 1: The regulatory timeline[17]

To the best of our knowledge the abovementioned laws have not been a subject of any systematic or comparative analysis with a focus on investment management. The proposed EU AI Act and GDPR are partial exceptions, as they have been extensively scrutinised (the former mostly by the industry, the latter by both the industry and academia[16]), but these analyses have always been standalone and not focused on the investment industry.

C. The Regulatory Perspective

The regulatory climate around AI-specific regulations (present and future) can be considered as cooperative and negotiated. Financial regulators wield substantial power following the 2008 financial crisis, while financial institutions—following multibillion taxpayer-funded bailouts and subsequent reputational fallouts—have limited appetite to take an aggressive or confrontational stance with the regulators.

Two primary uses of AI regulation can be distinguished: a technical and prudential approach; and a strategic approach. The technical and prudential perspective can be defined as rules and best practices in operations, conduct, and governance. The majority of regulations discussed in our Article fall under this category. Enforcement from the regulators can be expected. The strategic perspective can be defined as a set of fundamental principles (eg non-discrimination, non-harm,

[16] Eg S Ashour, 'Artificial Intelligence: A Roadblock in the Way of Compliance with the GDPR?', *Oxford Business Law Blog*, 2021; M Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27(2) *International Journal of Law and Information Technology* 91; J Gacutan and N Selvadurai, 'A Statutory Right to Explanation for Decisions Generated Using Artificial Intelligence' (2020) 28(3) *International Journal of Law and Information Technology* 193.

[17] Template courtesy of Microsoft: https://templates.office.com/en-us/project-timeline-with-milestones-tm00000009.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

beneficial outcomes for the general public). Those are guiding principles rather than rules per se. Their enforcement requires further concretisation.

The focus of this Article is on the regulatory considerations concerning AI adoption in investment management. Prosecution and enforcement considerations are in the realm of the existing legal process and are outside the scope of this Article. Liability is a key concern in financial services, and liability-related considerations will be highlighted as long as they arise or are affected by the use of AI. Attribution of liability when a product or service has multiple inputs or components from various parties can be complex and give rise to novel legal challenges which merit their own, separate research. In addition, there are different levels of regulatory scrutiny depending on the fund and client types. The primary point of reference for this Article is an individual retail investor and financial products available to them. The primary jurisdictional perspectives are the UK and the EU.

II. KEY HARD LAWS

Four key existing hard laws are currently relevant for the application of AI in investment management:[18]

1. Markets in Financial Instruments Directive ('MIFID II') and its Regulatory Technical Standard 6 ('RTS 6');[19]
2. Senior Managers and Certification Regime ('SM&CR');
3. General Data Protection Regulation ('GDPR'), which applies to AI insofar as AI uses personal data; and
4. European Union's proposed AI Act. While the AI Act is presently just a proposal (as opposed to all the other hard laws, which are already in force), it is the

[18] It could be argued that a list of regulations that can be applied to AI is longer (particularly given that most of financial regulation is—by design—technology-neutral and can be—also by design—interpreted quite broadly). For example, it could be argued that multiple general provisions (eg risk management- or market abuse-related) of the FCA Handbook can be applied to AI. After careful consideration we have decided to focus on regulations which have more direct relation or relevance to AI.

[19] In addition to MIFID II being implemented in its entirety into UK law (Financial Services and Markets Act 2000) the Financial Conduct Authority ('FCA') issued guidance titled 'Algorithmic Trading Compliance in Wholesale Markets' in February 2018. It does not add new provisions or requirements beyond what is already stated in MIFID II and RTS 6, but it elaborates on areas that are of particular interest to the FCA (defining algorithmic trading, development and testing, risk controls, governance and oversight, and market conduct). It is the only publication in our review which could not be clearly classified as either hard or soft law given that it is essentially an elaboration of MIFID II and RTS 6. We concluded that as the FCA report does not bring original substance to the body of regulations, it does not merit inclusion and discussion in our Article. Additionally, in September 2021 the European Securities and Markets Authority ('ESMA') issued a report titled 'MIFID II/MIFIR Review Report on Algorithmic Trading'. While the report is very detailed, we did not find its conclusions applicable to AI. The only relevant recommendation we found relevant pertains to RTS 6 whereby ESMA recommends certain refinements to the algorithm testing regime to ensure certain outcomes (eg no contribution to excess volatility).

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

first major regulation aimed specifically at artificial intelligence. It also establishes concrete regulatory requirements, which qualifies it as closer to a hard law than a soft law despite it being currently a non-binding proposal. Consequently, we chose to consider it on par with existing hard laws.

A. MIFID II and RTS 6

The most comprehensive piece of regulation applicable to EU- and UK-based investment managers is the Markets in Financial Instruments Directive ('MIFID II'), which is a 2018 novelisation of the original MIFID regulation from 2007. It is a comprehensive, harmonised legal framework for the investment industry. Suitability (ie suitability of a financial product for a specific individual's financial goals, constraints, and the level of financial literacy) is an essential part of MIFID II. It is also highly relevant when considering decisions made with the use of AI from the perspectives of transparency and explainability. MIFID II establishes several technical standards (Regulatory Technical Standards, 'RTS's) that expand certain provisions of MIFID II in greater detail. One of them (RTS 6) covers governance for trading and investment decision-making algorithms.

MIFID II is one of the key regulations in our analysis, because of its detailed provisions covering algorithmic trading. It is chronologically the first regulation to define best practices for algorithm oversight (in RTS 6), such as 'killswitches' and ongoing assessments. Interestingly (and arguably ahead of its time) both MIFID II and RTS 6 explicitly mention and briefly discuss not just trading algorithms, but also investment decision-making ones.[20] This is important because it signals to the industry that the directive considers algorithms in a broader sense, and not just in trading.[21]

B. SM&CR

While MIFID II lists rules applicable to investment management firms, SM&CR (Senior Management & Certification Regime) is a personal conduct regulation, focusing on accountability. The objective of SM&CR is a clear and unambiguous delineation of management chains and elimination of 'blind spots', ie business areas and business decisions no senior manager is clearly accountable for. SM&CR goes beyond the delineation of personal responsibility. It makes senior managers personally accountable (and potentially liable) for the actions of their teams and departments.

[20] The relevant part of RTS 6 reads: 'Investment decision algorithms make automated trading decisions by determining which financial instrument should be purchased or sold. Order execution algorithms optimise order-execution processes by automatic generation and submission of orders or quotes, to one or several trading venues once the investment decision has been taken. Trading algorithms that are investment decision algorithms should be differentiated from order execution algorithms having regard to their potential impact on the overall fair and orderly functioning of the market'.

[21] Based on our discussions in the investment as well consulting industries, we believe that this guidance has been noticed and noted in the industry as algorithms and AI began to proliferate outside the trading function.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

Given its singular focus on personal conduct ('fitness and propriety'), the SM&CR may initially seem irrelevant to the topic of AI regulation. However, decisions made by AI will always be made within specific (human) teams, business functions and ultimately human-run firms. Consequently, these decisions will always be attributed to a relevant senior manager. As stated explicitly by BoE's James Proudman in the 2019 speech[22] delivered at the FCA Conference on Governance in Banking: 'In the context of decisions made by machines which themselves learn and change over time, how do you define what it means for the humans in the firm to act with "reasonable steps" and "due skill, care and diligence?" […] Firms will need to consider how to allocate individual responsibilities, including under the Senior Managers Regime'.[23] Also, if senior managers' accountability did not apply to decisions made by AIs, then AI would become a way to circumvent SM&CR, leading to accountability 'blind spots', ie decisions with no human executive accountable for them.

C. GDPR

GDPR covers protection of personal data, usually referred to as Personal Identifiable Information ('PII'). Its main premise is to give individuals (which GDPR refers to as 'data subjects') control over how and by whom their personal data is collected, stored, and processed. GDPR is a high-profile regulation, mostly due to its impacts on lawfulness of collecting personal data online. As a technology-neutral regulation GDPR does not apply to AI directly—rather, it applies to personal data processed by AI. An AI algorithm could be fed PII and breach GDPR if data subjects have not consented. This could lead to substantial fines[24] as well as reputational damage. GDPR relates to AI on two levels, ie as regards the lawfulness of PII being fed to and processed by AI and as regards automated decision making, including profiling.

Automated decision making, including the right not to be subject to a decision based solely on it, is addressed in Article 22 GDPR. The right to an explanation[25] is covered in Article 15, with paragraph 15(h) specifically covering automated decision-making, including the right to 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'. Automated decision making and the right to explanation are arguably two aspects of GDPR most frequently discussed in the academic,

[22] J Proudman, Executive Director of UK Deposit Takers Supervision, Bank of England, 'Managing Machines: The Governance of Artificial Intelligence', 2019, https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/managing-machines-the-governance-of-artificial-intelligence-speech-by-james-proudman.pdf.

[23] SM&CR consists of two regimes: Senior Managers Regime and Certification Regime.

[24] EUR 20,000,000 or 4% of annual global turnover (whichever is higher).

[25] Information whether personal data concerning specific individuals is being processed, and if so, the purposes of the processing, the categories of personal data involved, the recipients of the data, data retention period, the right to request deletion of data, the right to lodge a complaint with a supervisory authority, source(s) of the data, and the existence of automated decision making.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

government, and professional spheres,[26] including some critical views regarding the extent and implications of the right to an explanation.[27]

Post-Brexit there are technically two GDPRs: EU GDPR and UK GDPR. The latter is no longer going to automatically align with the former. At the time of the writing of this Article, UK GDPR remains aligned with EU GDPR, however, there are indications from the UK lawmakers that the UK may review its data protection regime and potentially diverge from the EU GDPR blueprint in favour of a bespoke solution as highlighted in the May 2021 parliamentary report,[28] as well as in the September 2021 consultation.[29] Both documents prominently bring up Article 22 and automated decision making (including explicitly in the context of AI), with the former explicitly recommending that 'Article 22 of GDPR should be removed' and the latter concluding somewhat more softly that 'it is therefore important to examine whether Article 22 and its provisions are keeping pace with the likely evolution of a data-driven economy and society, and whether it provides the necessary protection'.

Furthermore, it is now clear that the European Parliament is planning a reform of GDPR, which incorporates lessons learned since the original GDPR was launched in 2018.[30] The European Parliament's position paper does not go as deep into recommendations on specific articles as the aforementioned British reports do, but it does explicitly bring up AI and concludes that the provisions of the current version of GDPR may be an obstacle to the development of European AI: 'Finding a legal ground for processing data in case of autonomous behaviour and for complying

---

[26] C Castets-Renard, 'Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making' (2019) XXX(1) *Fordham Intellectual Property, Media & Entertainment Law Journal* 91; L Tosoni, 'The Right To Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation' (University of Oslo Faculty of Law Legal Studies Research Paper Series, 14 May 2021); M Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-making and Data Protection in the Framework of the GDPR and Beyond' (2019 27(2) *International Journal of Law and Information Technology* 91; S Ashour, 'Artificial Intelligence: A Roadblock in the Way of Compliance with the GDPR?', *Oxford Business Law Blog*, 2021; HM Government, 'National AI Strategy', 2021; House of Lords Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?', 2018.

[27] L Edwards and M Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"' (2018) 16(3) *IEEE Security & Privacy* 46; L Edwards and M Veale, 'Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for' (2017–2018) 18 *Duke Law & Technology Review* 18; S Wachter, B Mittelstadt, and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law* 76.

[28] See Taskforce on Innovation, Growth and Regulatory Reform May 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf.

[29] See UK Government, 'Consultation Outcome: Data: A New Direction', 10 September, 2021, https://www.gov.uk/government/consultations/data-a-new-direction, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf.

[30] A Voss, 'Fixing the GDPR: Towards Version 2.0', *EPP Group*, 25 May 2021, https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

with the information duties as well as the transparency, accountability and explainability principles of the GDPR is also a decisive challenge for developers and operators of AI-systems'.

D. The EU AI Act Proposal

Published in April 2021, the European Commission's AI Act proposal is the first regulation in the world to focus exclusively on AI issued by a major regulatory body. For the avoidance of doubt, it is still a proposal, thus it is not binding and is subject to change before it is enacted.[31] The AI Act is a generalist regulation, not focusing on one specific sector, though its impact on financial services will likely be substantial. As a consequence of it being the first regulation of its kind (and a very high-profile one) it is also likely to become a primary reference for future AI regulations in various jurisdictions worldwide. As such, the significance of the AI Act cannot be overstated.

The EU has followed a risk-based approach to AI,[32] considering riskiness from the perspective of use cases and industries (a horizontal approach) and ensuring its compatibility with existing EU regulations, including GDPR. The AI Act focuses on prohibited[33] and high-risk[34] AI systems and applications. It provides additional rudimentary guidance for 'systems intended to interact with natural persons' (Article 52). The remainder of AI systems would be left unregulated had it not been for Article 69, which recommends that operators of all other types of AI voluntarily observe the same principles as high-risk systems.

The position of financial services in the Act is somewhat ambiguous. The explanatory memorandum lists finance as one of the 'high-impact sectors', but the explicit list of high-risk systems in Annexes II and III of the AI Act does not include financial services. The AI Act itself explicitly references credit institutions (ie banks) in multiple articles. The Act explicitly references credit scoring as a high-risk application, but 'credit score' itself is not clearly defined in the regulation. The AI Act lists 'access to financial resources or essential services such as housing, electricity, and telecommunication services' as being determined by the credit score, which implies

---

[31] Cf W Buczynski, 'The EU Artificial Intelligence Act and Financial Services', *CFA Institute Enterprising Investor Blog*, 6 April 2022, https://blogs.cfainstitute.org/investor/2022/04/06/the-eu-artificial-intelligence-act-and-financial-services.

[32] We note that the EU's risk-based approach seems to be closely inspired by the 'risk-adapted regulatory system for the use of algorithmic systems' proposed in 2019 by the German Data Ethics Commission, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=2.

[33] Prohibited applications of AI: subliminal manipulation; exploitation of vulnerable persons and groups; social credit scoring; and real-time biometric identification in public spaces (with certain exceptions for law enforcement purposes).

[34] The list of high-risk systems is much longer, and itemised in annexes II and II of the EU AI Act, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF. It does not include the financial services industry per se, and focuses mostly on industries and situations that can have an immediate and severe impact on a person's health, wellbeing, and fundamental rights, such as civil aviation, toys, radio equipment, medical devices, automotive vehicles, railways, biometric identification, employment, and public benefits.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

a broader interpretation than typical credit scoring used by commercial entities for ascertaining loan or credit card eligibility.

Similar to the GDPR, non-compliance with the EU AI Act carries the risk of substantial monetary penalties[35]—in extreme cases higher than the maximum penalties applicable under the GDPR.

III. KEY REGULATORY THEMES

A. *Overview*

Our thematic analysis covers all hard and soft laws as listed in Appendix 2. It needs to be noted that the themes most prevalent in existing laws may or may not turn out to be the most pertinent ones. Given the nascent state of AI regulation, it is at least theoretically possible that presently unforeseen or underappreciated considerations may turn out to be critical in the future.

There is obviously a degree of discretion in any aggregation process.[36] To allow for meaningful aggregation, the themes need to be relatively broad, with the focus on meaning and outcomes rather than arbitrary labels. The objective is not some sort of definitive ranking but rather a comprehensive 'landscape' (list) of regulatory themes with an indication of their prevalence.

We identified 17 themes[37] and grouped them into three categories (see Table 1): (1) technology; (2) governance; and (3) business and conduct.

Please note that ethics-focused guidances and ethics-related themes have been excluded as they merit separate research. While we recognise the fundamental importance of ethics in financial services, as well as ethics of AI, the focus of this paper is on the tangible and actionable aspects of soft and hard laws.

Table 2 ranks the regulatory themes by popularity in the hard and soft laws analysed.

B. *Highlights*

Many of the top themes come as expected: transparency, data-drivenness and explainability. Their popularity is representative of the key points in the industry discussions on safe and responsible adoption of AI.[38]

---

[35] Up to EUR 30,000,000 or 6% of the global annual turnover (whichever is higher). Interestingly, poor data governance could trigger the same fine as engaging with outright prohibited practices.

[36] Morley et al experienced a similar challenge when reviewing and aggregating AI ethical frameworks, https://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC7417387&blobtype=pdf. They referred to their aggregated framework as a 'fragile consensus' because 'there are gaps across the different sets of principles and all use slightly different terminology, making it hard to guarantee that the exact same meaning is intended in all cases'. We avoided that fragility in our framework by allowing themes to be broad and by not aiming to reduce their count to some arbitrary number (eg 3, 5, or 10).

[37] To count as a theme, the same concept needed to appear in at least two separate regulatory publications.

[38] These themes were at the forefront of such high-profile industry events as the 16–17 July 2019 'AI Ethics in the Financial Sector' conference jointly organised by the Financial Conduct Authority and the

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

Table 1: Regulatory themes

	Theme	Category
1	Data-drivenness/reliance/quality	
2	Opacity/transparency	
3	Auditability/reproducibility/explainability	
4	(Cyber)security/vulnerability	Technology
5	Autonomy/agency	
6	Complexity/emergent behaviours/interconnectedness	
7	Technology neutrality	
8	Personal data protection/privacy	
9	Algorithm governance: pre-deployment testing/periodic assessment/ongoing monitoring	
10	Reliance on third parties/outsourcing	
11	Disclosures of AI use	Governance
12	Algorithm inventory	
13	Risk-based approach/proportionality	
14	Senior management accountability	
15	Internal skills (esp compliance)	Business/
16	Market abuse	Conduct
17	Suitability/knowledge of investment products offered	

Table 2: Regulatory themes by popularity

Opacity/transparency	**12**
Personal data protection/privacy	**11**
Data-drivenness/reliance/quality	**11**
Auditability/reproducibility/explainability	**10**
Internal skills (esp compliance)	**9**
Complexity/emergent behaviours/interconnectedness	**9**
(Cyber)security/vulnerability	**9**
Algorithm governance: pre-deployment testing/periodic assessment/ongoing monitoring	**9**
Senior management accountability	**7**
Technology neutrality	**7**
Reliance on third parties/outsourcing	**7**
Risk-based approach/proportionality	**6**
Market abuse	**6**
Disclosures of AI use	**5**
Algorithm inventory	**4**
Autonomy/agency	**4**
Suitability/knowledge of investment products offered	**2**

(F'note continued)

Alan Turing Institute, https://www.turing.ac.uk/events/ai-ethics-financial-sector; the 7 February 2020 University College London seminar 'Translating Algorithm Ethics into Engineering Practice', http://govtechlab.org/seminar-translating-algorithm-ethics-into-engineering-practice-ucl-digital-ethics-forum; or The Investment Association events 'Data Science and AI in Investment Management', 15 September 2020, https://www.theia.org/events-training/webinars/techtalk-data-science-and-ai-

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

Personal data and security are major standalone considerations, which have been very high-profile for several years, even pre-dating the recent breakthroughs in AI. The very high ranking of personal data protection is likely attributable to GDPR, the impacts of which have been felt globally, and which inspired similar data protection regulations worldwide. Multiple aspects of cybersecurity have been prominent since financial services started getting increasingly digitalised around the early 2000s. However, secure AI means more than ensuring best possible cybersecurity defences against intrusion or theft. While those certainly apply, there are additional, considerations unique to AI which are discussed in greater detail in Section III.C.4 below. While neither personal data protection nor cybersecurity are unique or new to AI, they lead to new interplays and dependencies that need to be addressed by the regulators. It could be argued that they are also complementary: security implicitly covers all the non-personal data and other intellectual property of the investment firm that does not otherwise fall under personal data protection. Their popularity thus comes as no surprise.

The high popularity of internal skills and algorithm governance is noteworthy, as those themes are not equally prevalent in the popular discourse, although they figure largely in the industry discussions. The high popularity of internal skills is likely reflective of a wider AI skills shortage in the investment industry, which is a widely acknowledged issue with no simple or immediate solution. The high popularity of algorithm governance also indicates that regulators have given AI governance thorough consideration and it has been addressed from the industry-specific perspective.

The relatively high popularity of managerial accountability might be attributable to the passing of the SM&CR, which, like the GDPR in the realm of personal data, made impacts beyond the jurisdiction it applies to. Furthermore, management accountability has been a regulatory grey area for many years (much like personal data protection before the GDPR), so it is possible that the SM&CR is acting as a catalyst to a much wider adoption of management accountability regimes. Alternatively, it is possible that regulators considered managerial accountability to pre-emptively disambiguate the potential issue of a regulatory 'blind spot' whereby there would be no human accountable for actions or decisions made by a seemingly autonomous AI.

Disclosures of AI use were one of the less-expected themes (the other being technology-neutrality). Legal disclosures are a core part of any fund's documentation, however technological disclosures, let alone mandatory ones, are less prevalent in the public discussion.

The very low rank of suitability is surprising given that it is a critical consideration in investment management. One plausible explanation could be that most regulators regarded it as a non-technical consideration which is sufficiently addressed in existing regulations.

(F'note continued)

investment-management) and Artificial Intelligence in Investment Management', 17 November 2021, https://www.theia.org/events-training/webinars/artificial-intelligence-investment-management.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

C. Technology

1. Data-drivenness/reliance/quality

Present-day AI systems learn from extensive datasets. If the underlying data is flawed then the results will also be flawed (a situation colloquially referred to as 'garbage in, garbage out'). Data can be scrutinised from the perspective of quality, accuracy, completeness, relevance, and timeliness. In combination, these technical attributes can inform higher-level, 'soft' attributes such as bias or discrimination.

Multiple regulations feature detailed guidelines on data and data governance (eg the EU AI Act [Article 10]) or RTS 6; also Art. 3.23 of the Model AI Governance Framework is comprehensive and applicable to financial services). When using third-party data (eg large sets of market data provided by commercial vendors) the financial institution remains responsible and accountable. That is in line with the basic tenet of outsourcing, whereby an organisation cannot outsource its regulatory responsibilities.[39]

Data considerations overlap with GDPR. It is not a full overlap, as GDPR covers personal data only, while the types of data financial AIs work off will vary and are likely to include non-personal data (eg market data or news sentiment). There is also the issue of uncertain causation in the context of liability (discussed in the EU's 'Liability for AI and Other Emerging Digital Technologies' report). The report points out that an AI malfunction can be caused either by the underlying data being flawed, or the data being imperfectly processed by the AI system, making liability challenging to attribute.

2. Opacity/transparency

Regulations convey the same message in different ways: either as importance of transparency or as risks and disadvantages of opacity. Transparency is frequently considered self-explanatory; it is also often used synonymously with explainability. Following an in-depth discussion by Hacker,[40] we use the following definitions. The term transparency describes how easily an algorithm can be understood. The term explainability (interpretability) signals how easily an outcome of an algorithm can be explained.[41] It is therefore possible for an AI system to be transparent and yet not be explainable. The definition of transparency can be broadened to include relevant stakeholders having access to relevant information about a given AI system.[42]

---

[39] Cf European Banking Authority (EBA) Guidelines on Outsourcing Arrangements (which, despite its name, is a legally binding obligation) Title III, Chapter 6, Art 35 states clearly: 'The outsourcing of functions cannot result in the delegation of the management body's responsibilities'.

[40] P Hacker, R Krestel, S Grundmann, and F Naumann, 'Explainable AI under Contract and Tort Law: Legal Incentives and Technical Challenges' (2020) 28 *Artificial Intelligence and Law* 415.

[41] Cf R Roscher, B Bohn, M F Duarte, and J Garcke, 'Explainable Machine Learning for Scientific Insights and Discoveries', *IEEE Access*, 24 February 2020 (for a further discussion).

[42] F Ostmann and C Dorobantu, 'AI in Financial Services', *The Alan Turing Institute*, 2021, https://www.turing.ac.uk/sites/default/files/2021-06/ati_ai_in_financial_services_lores.pdf.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

The two concepts, while not synonymous, are complementary and intertwined. Transparency is a key aspect of algorithm governance. Transparency is about the financial firm having a full understanding of its AI and algorithms and understanding how the outcomes are produced. Explainability is about the outcomes themselves, which relates not just to the financial institution, but first and foremost to the clients. Transparency is the most popular theme on our list, and it interplays with other themes (not just explainability). As IOSCO points out, it is closely linked with AI disclosures. ICO's 'Explaining Decisions Made with AI'[43] makes the same point in the context of personal data.

Transparency is a nuanced and complex concept in the context of financial services. Florian Ostmann and Cosmina Dorobantu elegantly condense it down to three main aspects: system transparency, process transparency, and relevant stakeholders. System transparency captures the logic of the system itself, ie how (and what) inputs get processed to generate outputs. Fully deterministic systems are by definition fully transparent in this regard. It may not always be possible for an AI to have such a level of transparency, but it should at least be fully transparent with regards to inputs used and their percentage weights and other internal relationships. In our view, AI systems in investment management should be designed and developed with maximum transparency as one of the key objectives. Process transparency covers all remaining technical, operational, and business aspects of the AI system throughout its lifecycle: from design via deployment and ongoing oversight through to eventual decommissioning. Stakeholders are consumers of system and process transparency information and make their decisions on the basis on this information. IOSCO points out that there should be different levels of transparency depending on the stakeholder and warns about the dangers of 'excessive transparency' if it opens the system to exploitation or manipulation.

Article 24(2) MIFID II puts on the investment firm the requirement to 'understand the financial instruments they offer or recommend'.[44] An opaque, non-explainable investment-picking AI would violate this requirement (interestingly, RTS 6 does not mention transparency at all). It can be argued that SM&CR indirectly requires transparency of AI systems from the perspective of management accountability as it seems implausible from the business and legal perspectives that senior managers would readily accept accountability for decisions that they cannot fully understand.

Transparency is also one of the fundamental principles of GDPR: from data collection to processing, and it is mentioned throughout the regulation. Even though GDPR does not apply universally to AI (it only applies when PII is being processed), transparency being mentioned so prominently elevates its importance and significance given GDPR's high profile as a regulation (also outside the EU).

---

[43] Information Commissioner's Office, 'Explaining Decisions Made with AI', 2020.

[44] MIFID II does not state this explicitly, but in this context 'instruments' means 'funds' (ie collective investment schemes, consisting of multiple holdings) rather than individual equities or bonds. The investment manager is still required to understand the nature and characteristics of all the holdings in their portfolio, because without understanding the constituents, they would not be able to understand the portfolio as a whole.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

The proposed EU AI Act features provisions on transparency and provision of information to users (Articles 13 and 52), but in our view transparency remains an under-addressed area of the Act. Article 13 mentions it in a single paragraph, whereas Article 52 has very limited scope, focusing on the 'emotional' interactions between AIs and humans. The absence of comprehensive provisions regarding transparency in the EU AI Act is notable.

Looking at EU hard laws collectively, the observation is that none of them comprehensively puts transparency requirements on AI systems, leaving a regulatory gap. If this is unintentional, then hopefully future versions of the EU AI Act will add explicit provisions regarding transparency. The 'Report on Safety and Liability Implications of AI, the Internet of Things and Robotics' appears to corroborate our conclusions by stating: 'The Union product safety legislation does not explicitly address the increasing risks derived from the opacity of systems based on algorithms. It is therefore necessary to consider requirements for transparency of algorithms'.

The UK will not be bound by the EU AI Act, but it is expected to come up with its own regulations, likely based on the July 2022 proposal,[45] where transparency is one of the prominent themes. In addition, it is expected that the UK will have some form of financial services-specific AI regulation. This expectation is based on a discussion paper[46] published jointly by the BoE and the FCA in October 2022, where transparency is one of the relevant themes.

The final and arguably critical aspect of transparency is the regulatory one. Even in the absence of explicit AI regulations, regulators can request and reasonably expect information on AI systems, their logic, safety, governance, robustness, etc from their regulated firms. It is highly likely that transparency would be one of the key areas of regulators' interest due to its potential risk management implications and client impacts.[47] Failure to satisfy this request could lead to escalated regulatory action(s) and reputational impacts.

3. Explainability/auditability/reproducibility

AI systems should be engineered and configured in such a way that their outcomes are explainable (and thus understandable) to the financial institution, but most

[45] UK Government, 'Policy Paper: Establishing a Pro-innovation Approach to Regulating AI, 18 July 2022, https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai.

[46] Bank of England Discussion Paper, 'DP5/22 – Artificial Intelligence and Machine Learning', 11 October 2022, https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence.

[47] In the UK, such requirement could be based on FCA Principles, https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html, particularly Principles 2 ('A firm must conduct its business with due skill, care, and diligence') and 3 ('A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems').

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

importantly to the clients. Ideally, the causality of decisions and outcomes should be clearly auditable.

The German regulator, BaFin, states explicitly that financial institutions should be responsible for ensuring explainability of AI decisions. It goes as far as to say that 'supervisory authorities will not accept any models presented as an unexplainable black box'.[48] Taken literally, this would preclude the use of deep learning methods, which have led to recent progress in machine learning applications such as speech or vision. BaFin notes that there may be two levels of explainability: general explainability of a model; and specific explainability of an outcome applicable to a particular individual.

The UK's Information Commissioner's Office ('ICO') has given explainability thorough consideration in its 'Guidance on the AI Auditing Framework Draft Guidance for Consultation'.[49] It notes the dilemma of having to trade off explainability for statistical accuracy and vice versa. Both BaFin and ICO propose simplification of the models (ie using simpler, explainable models instead of complex, 'black box' ones) as a solution for transparency (although ICO does permit 'black box' models in certain circumstances). ICO has further expanded on the topic in 'Explaining Decisions Made with AI', which is solely dedicated to different aspects of explainability. ICO identifies six ways of explaining AI decisions, which are: rationale explanation; responsibility explanation; data explanation; fairness explanation; safety and performance explanation; and impact explanation.[50] ICO has researched explainability more comprehensively than any other regulatory body and their six-part model can be considered a regulatory gold standard. ICO strongly encourages 'operationalising' explainability through introduction of dedicated policies and procedures.

---

[48] BaFin, note 15 above.

[49] Information Commissioner's Office, 'Guidance on the AI Auditing Framework Draft Guidance for Consultation', 2020.

[50] Information Commissioner's Office, 'Guide to Data Protection', https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence/part-1-the-basics-of-explaining-ai/what-goes-into-an-explanation:

'- Rationale explanation: the reasons that led to a decision, delivered in an accessible and non-technical way.
- Responsibility explanation: who is involved in the development, management and implementation of an AI system, and who to contact for a human review of a decision.
- Data explanation: what data has been used in a particular decision and how.
- Fairness explanation: steps taken across the design and implementation of an AI system to ensure that the decisions it supports are generally unbiased and fair, and whether or not an individual has been treated equitably.
- Safety and performance explanation: steps taken across the design and implementation of an AI system to maximise the accuracy, reliability, security and robustness of its decisions and behaviours.
- Impact explanation: steps taken across the design and implementation of an AI system to consider and monitor the impacts that the use of an AI system and its decisions has or may have on an individual, and on wider society'.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

4. *(Cyber)security/vulnerability*

Whether an AI system is built and hosted in-house or is built using third-party components and hosted in the cloud (which is frequently the case), it constitutes the property of the financial organisation. Any attempt to copy or disrupt the system would require penetration of the company's IT infrastructure (even if it is outsourced), which would likely constitute a criminal offence covered by existing laws.[51] In addition to these standard cybersecurity considerations, which have existed for decades, there are more unique and AI-specific risks, such as: (1) Reliance on 'as is' open-source components or libraries, which can be hacked or otherwise compromised.[52] Due to their very nature open-source tools may lack the support infrastructure needed to address hacks or vulnerabilities as quickly and robustly as commercial tools; (2) reliance on commercial software and services that can be hacked or otherwise compromised;[53] (3) intentional 'poisoning' of the training data to destabilise the model;[54] (4) theft of training data (which can be confidential, personal, and used to train another model without the work and time it takes to prepare quality training data); (5) various ways of reverse-engineering the model by analysing its outputs based on known inputs (model inversion,[55] 'algo-sniffing'[56]); and (6) theft of the model itself.[57]

Please note that only some of the abovementioned cyber risks are illegal (eg theft). Some are technically legal, although questionable from an ethical perspective (algo-sniffing), and some are known technology risks (reliance on open-source components). The list above is not exhaustive. It is likely that as AI is being widely implemented, previously unforeseen cyber threats arise. This should not affect the overall approach to cybersecurity, with the focus being protection of the client data as well as the investment firms' intellectual property.

---

[51] Eg under the Computer Misuse Act 1990 ('CMA') in the UK.

[52] P H O'Neill, 'The Internet Runs on Free Open-Source Software. Who Pays to Fix It?', *MIT Technology Review*, 17 December 2021, https://www.technologyreview.com/2021/12/17/1042692/log4j-internet-open-source-hacking; S Vaughan-Nichols, 'When Open-Source Developers Go Bad', *ZD Net*, 13 January 2022, https://www.zdnet.com/article/when-open-source-developers-go-bad.

[53] L H Newman, 'No One Knows How Deep Russia's Hacking Rampage Goes. A Supply Chain Attack Against IT Company Solarwinds Has Exposed as Many as 18,000 Companies to Cozy Bear's Attacks', *Wired*, 14 December 2020, https://www.wired.com/story/russia-solarwinds-supply-chain-hack-commerce-treasury.

[54] R S S Kumar, D O'Brien, J Snover, K Albert, and S Viljoen, 'Failure Modes in Machine Learning', 2019, https://docs.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning.

[55] M Veale, R Binns, and L Edwards, /Algorithms that Remember: Model Inversion Attacks and Data Protection Law', *Philosophical Transactions of The Royal Society A*, 2018.

[56] D Mackenzie, 'How to Make Money in Microseconds' (2011) 33(10) *London Review of Books* 16; BDO UK, 'Achieving Best Execution: Are AI-Powered Smart Order Routers the Gold Standard?', 21 September 2021, https://www.bdo.co.uk/en-gb/insights/tax/innovation-and-research-and-development-tax-incentives/achieving-best-execution-are-ai-powered-smart-order-routers-the-gold-standard.

[57] F Tramèr, F Zhang, A Juels, M K Reiter, and T Ristenpart, 'Stealing Machine Learning Models via Prediction API' (2016) *Proceedings of the 25th USENIX Security Symposium*.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

Cybersecurity is the most consistent theme in terms of importance, risks, and overall message.

5. *Complexity/emergent behaviours/interconnectedness*

Complexity is both a feature and a risk, as complex systems may be difficult to understand, and their potential malfunctioning may not be easily and immediately spotted. Interconnectedness is also both a feature (AI systems are rarely completely standalone, and they exist within a highly interconnected financial ecosystem) and a risk (contagion). Emergent behaviours are not part of the original programming and only arise when various systems are connected.[58] Emergent behaviours in the context of financial AI can be defined as new behaviours arising when AI systems begin to interact with other systems.[59] Consequently, complexity relates mostly to systemic considerations, as opposed to most other themes, which are implicitly applicable on individual company (or even application) level. The aspect of 'unforeseen-ness', in combination with a potentially broad impact is what makes complexity a critical theme as AI becomes pervasive in financial services. This applies particularly to those activities where it interacts with the broader market, such as trading.

BaFin recommends starting an international discussion on the definition and measurement of interconnectedness. It points out that 'closely interconnected systems are susceptible to the rapid and uncontrolled spread of disruptions'.[60] PBOC looks at AI from the perspective of market stability and warns against homogenization of algorithms, which could lead to herding. It mandates financial institutions to develop plans for such eventuality, up to and including 'manual interventions', and even termination of the AI system.[61] FSB highlights 'new and unexpected forms of interconnectedness' as a potential implication of growing adoption of AI. Greater interconnectedness could help share risks, but also exacerbate them in a herding scenario. FSB also warns against 'unintended, and possibly negative' consequences of complex AI systems interacting in the market, using trading as an example.[62]

Two publications of the European Union ('Liability for Artificial Intelligence and Other Emerging Digital Technologies' and 'Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics') point out how increasing complexity of AI systems might complicate establishing liability. The former points out that interconnectedness may lead to difficulties in predicting

[58] C W Johnson, 'What Are Emergent Properties and How Do They Affect the Engineering of Complex Systems?', *Department of Computing Science, University of Glasgow*, http://www.dcs.gla.ac.uk/~johnson/papers/RESS/Complexity_Emergence_Editorial.pdf.

[59] S Sheikh-Bahaei, 'The E-Dimension: Why Machine Learning Doesn't Work Well for Some Problems?', *Data Science Central*, 7 June 2017, https://www.datasciencecentral.com/the-e-dimension-why-machine-learning-doesn-t-work-well-for-some.

[60] BaFin, note 15 above.

[61] People's Bank of China, note 13 above.

[62] Financial Stability Board, note 9 above.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

performance. At present, complexity appears to be a somewhat abstract consideration, which may explain why it is not mentioned as prominently as more immediate considerations.

6. *Autonomy/agency*

Autonomy is defined as the ability to self-govern.[63] Autonomy is not binary: there are gradients between fully autonomous and fully controlled.[64] For the avoidance of doubt, fully autonomous AI is one that takes action with no immediate human oversight (eg AI-powered high frequency trading, which due to the sheer speed of trading decisions would be fully autonomous). Fully controlled AI is one whose output serves as an input for a human decisionmaker, and can be analysed, reviewed, and even completely rejected.

Autonomy is explicitly mentioned only in two publications ('Liability for Artificial Intelligence and Other Emerging Digital Technologies' and 'Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics'—both from the European Commission). Both discuss autonomy mostly from the perspective of product safety and liability. Of those two perspectives, only liability applies to financial services. The real concern with autonomy is unforeseen and unintended consequences of actions taken by an autonomous AI system with direct market access. While we have no knowledge of such actions taken by AI, adverse situations caused by non-AI algorithms did arise in the past.[65] Depending on the perspective, autonomy might seem an exotic, futuristic consideration, or a plausible high-impact event, which the regulators have not sufficiently considered. Our view is the latter. Regulators should give serious consideration to autonomy of AI systems and mandate risk-minimizing procedures (including discouraging deployment of fully autonomous AIs, particularly as regards market access).

---

[63] Merriam-Webster Dictionary, 'Autonomy', https://www.merriam-webster.com/dictionary/autonomy.

[64] Autonomous driving research provides a useful framework to start from (cf C Rödel, S Stadler, A Meschtscherjakov, and M Tscheligi, 'Towards Autonomous Cars: The Effect of Autonomy Levels on Acceptance and User Experience' (2014) *AutomotiveUI '14: Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*), although the spectrum of autonomy for financial AIs may turn out to be less discrete and more continuous than in self-driving cars.

[65] The 28 May 2021 edition of FCA's Market Watch (67) includes a section titled 'Addressing Potentially Poorly Designed Algorithms', which reads: 'Our internal surveillance algorithms identified trading by an algorithmic trading firm which raised potential concerns about the impact the algorithms responsible for executing the firm's different trading strategies were having on the market. As a result of our enquiries, the firm adjusted the relevant algorithm and its control framework to help avoid the firm's activity having an undue influence on the market'. While this is just a single occurrence, we are aware of past high-profile systemic impacts of (non-AI) algorithmic trading, such as the Flash Crash of 2010 or the USD 440m trading loss incurred by (now defunct) Knight Capital.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

7. *Technology neutrality*

Technology neutrality has been a default approach to financial regulation. A handful of regulations (GDPR, PDPC, BaFin) address it explicitly. GDPR clearly states that 'the protection of natural persons should be technologically neutral and should not depend on the techniques used', which is echoed by BaFin and PDPC. By contrast, OECD notes that a technology-neutral approach to financial regulation may be challenged by some AI use cases. SM&CR, due to its nature, is genuinely technology-neutral even though it lists algorithmic trading as one of its covered areas. PDPC[66] provides an interesting discussion of different types of neutrality, which it refers to as 'agnosticism'.

Technology neutrality can be interpreted in various ways. Non-AI-specific laws tend to focus on activities, actions, and outcomes (eg SM&CR, MIFID II), with technology being the means to deliver those, so they are technology-neutral in that sense. AI-specific regulations can be technology-neutral in a narrower sense, by focusing on a specific technology, but not defining it to the level of engineering detail (eg this is how the proposed EU AI Act defines technology neutrality). We call this approach 'technique neutrality'. Technique neutrality helps regulators avoid prescriptiveness, which could give rise to loophole-seeking and regulatory arbitrage. It also ensures that regulations, once enacted, maintain their relevance for longer.

D. Governance

1. *Personal data protection/privacy*

Personal data protection, as well as broader data protection and privacy, have been a fundamental consideration since GDPR was enacted (April 2016). While the GDPR is an EU regulation, it has a global effect through at least two mechanisms. Firstly, data transferred to a third country is protected via the adequacy requirement (Article 45): non-EU countries need to be certified (and thus effectively compliant) to allow transfer of EU data. The certification is not mandatory, but lack of it becomes hugely limiting for the third country from the perspective of international business. As a consequence of Article 45, the GDPR becomes a de facto international regulation. Secondly, the GDPR has shaped best practice. It has been quickly appreciated worldwide, becoming a reference point for data protection laws in other jurisdictions[67].

---

[66] Personal Data Protection Commission, 'Model Artificial Intelligence Governance Framework (2nd ed)', Singapore, 2020.

[67] Since GDPR has been enacted, similar data protection regulations emerged in the US (in California (CCPA), Virginia (CDPA), Utah (UCPA), Connecticut (An Act Concerning Personal Data Privacy and Online Monitoring), and Colorado (CPA)), in Brazil (Law 13.709), Abu Dhabi (Data Protection Law No. 5), and the Republic of South Africa (POPIA). India and China are working on their own personal data protection laws (PDPB and PIPL, respectively).

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

2. *Algorithm governance*

Algorithm governance covers various activities and controls spanning the entire lifecycle of an algorithm. It appears in a number of regulations (eg PBOC's 'Guiding Opinions', PDPC's 'Model Artificial Intelligence Governance Framework', IOSCO's 'The Use of Artificial Intelligence and Machine Learning By Market Intermediaries and Asset Managers'—but most comprehensively in RTS 6). The objective is ensuring that the algorithm is well-calibrated and supervised throughout its lifecycle.

Based on the above, a well-implemented governance framework should ensure that: (1) the algorithm is thoroughly tested pre-deployment; (2) it is periodically retrained on the most recent available data; (3) it does not 'drift' (ie the relationship between input and output data does not change); (4) it is regularly assessed for viability as opposed to running indefinitely; (5) there is human oversight ('human in the loop'—ideally on real-time basis); (6) there are clear parameters and limits on the types of instruments, sizes of the trades, trading venues, etc the algorithm may trade; (7) material post-deployment changes to the algorithm are tested and documented; and (8) the algorithms are all inventoried and accounted for.

There is a precedence to algorithm governance in the form of model[68] governance (sometimes also referred to as model risk management). In the UK, the FCA conducted a thematic review in 2015,[69] followed by a comprehensive consultation paper published by the Bank of England and Prudential Regulatory Authority setting out expectations regarding model risk management.[70] In the US, the Federal Reserve has issued regulatory guidance SR 11-7 on model risk management.[71] SR 11-7 is similar to RTS 6—the former is more conceptual and theoretical, while the latter is more prescriptive and technical.

3. *Reliance on third parties/outsourcing*

Outsourcing is neither novel nor specific to AI. Since financial services organisations started migrating to the cloud *en masse* in the 2010s, outsourcing became more prominent. By around 2017 (as 'cloud-first' became the default approach in the industry),

---

[68] Models and algorithms are not synonymous. An algorithm is a 'systematic procedure that produces—in a finite number of steps—the answer to a question or the solution of a problem'. A model is a 'physical, conceptual, or mathematical representation of a real phenomenon that is difficult to observe directly' (in finance, this definition stretches to 'impossible to observe directly' in such instances as worst-case scenarios in risk modelling). Those two definitions may sound similar, but models and algorithms are usually unambiguously distinguishable (eg the Monte Carlo simulation attempts to model in a simplified form hypothetical real-world scenarios, but it is not an algorithm). It would therefore seem inconsequent to carefully oversee the models whilst leaving algorithms ungoverned or loosely governed.

[69] Financial Conduct Authority, 'Structured Products: Thematic Review of Product Development and Governance', 2015.

[70] Bank of England, 'CP6/22 – Model Risk Management Principles for Banks,' https://www.bankofengland.co.uk/prudential-regulation/publication/2022/june/model-risk-management-principles-for-banks.

[71] Federal Reserve, 'Supervisory Guidance on Model Risk Management', 2011.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

outsourcing has risen to the top of the agenda in many financial institutions. Regulators recognised the impacts of cloud outsourcing and started issuing soft[72] and hard[73] laws around it. It marked the first time that regulators focused on a specific technology and began regulating it (thus making an exception from their standard technology-neutral approach).

AI is likely to be outsourced in two ways: firstly, through the use of third-party technology (from public domain tools and libraries such as TensorFlow to 'commoditised' AI solutions from enterprise vendors such as Google, Microsoft, or Amazon Web Services [AWS]); secondly, through the use of third-party infrastructure. Large cloud vendors such as Google, Microsoft, or AWS offer suites of customisable and scalable AI solutions, which by default run on their respective cloud infrastructures.

AI is therefore likely to fall under existing regulations on cloud outsourcing and all the considerations they entail (eg legal, contractual, risk management, downstream outsourcing, data location, oversight of the cloud provider, exit plans, data protection, cybersecurity, etc).

In addition to pure outsourcing considerations, there are also systemic ones. If multiple financial service providers rely on solutions from a handful of leading cloud vendors, running on those vendors' infrastructures introduces novel systemic risk into the financial system as a whole.[74]

4. Disclosures of AI use

Certain soft laws (eg IOSCO's 'The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers', PDPC's 'Model Artificial Intelligence Governance Framework', PBOC's 'Guiding Opinions') propose that financial institutions disclose their use of AI. The proposals are neither very detailed nor uniform. IOSCO and PBOC propose mandatory disclosures (although not identical: IOSCO proposes disclosures to the regulator as well as the clients; PBOC only proposes the former); PDPC merely encourages them. The exact scope and level of detail are not stated, although all regulations seem to focus primarily on instances of AI where there are direct client impacts.

---

[72] Financial Conduct Authority, 'FG 16/5 Guidance for Firms Outsourcing to the "Cloud" and Other Third-Party IT Services', 2019.

[73] Commission de Surveillance du Secteur Financier ('CSSF'), 'Circular CSSF 17/654 IT Outsourcing Relying on a Cloud Computing Infrastructure', 2019; BaFin, 'Guidance on Outsourcing to Cloud Service Providers', 2018; Monetary Authority of Singapore (MAS), 'Guidelines on Outsourcing', 2018; Securities and Futures Commission ('SFC'), 'Circular to Licensed Corporations - Use of External Electronic Data Storage', 2019; EBA, 'Final Report on EBA Guidelines on Outsourcing Arrangements', 2019.

[74] Some financial regulators (eg Bank of England or Prudential Regulation Authority) signal their plans to increase scrutiny of cloud services providers given their systematic importance for the financial services industry. 'Bank of England Sees Potential Risks from Cloud Data Providers', *Reuters*, 21 April 2021, https://www.reuters.com/business/finance/boe-might-need-stronger-tools-tech-rise-fintech-ramsden-2021-04-21.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

5. *Algorithm inventory*

MIFID II requires that algorithmic trades be flagged so that they can be clearly distinguished and that firms engaged in algorithmic trading notify their local authorities which trading venues they trade on. The directive also gives national authorities the power to request details of algorithmic trading strategies from regulated firms on an ad hoc basis. Consequently, regulated firms need to keep a detailed and up-to-date inventory or registry of these algorithms to meet this regulatory requirement.

Algorithm inventory requirements appear in only a handful of regulations, and always implicitly. Besides MIFID II, there is an implied requirement in IOSCO's 'The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers', while BaFin[75] talks about examining AI in models subject to supervisory approval. Having an algorithm inventory is very closely related to algorithm governance. It is also essential to be able to comply with AI disclosure requirements. It can be argued that all regulations addressing algorithm governance or AI disclosures require having algorithm inventories by default.[76]

Setting up and maintaining algorithm inventories also requires new, interdisciplinary overlaps in terms of teams and business functions. While algorithm governance is likely to be in the remit of technology teams, algorithm inventory is likely to sit at the intersection of operational risk, compliance, regulatory reporting, and technology, requiring collaboration of teams that may not have previously worked closely together.

6. *Risk-based/proportionate approach*

The European Union's definition of the proportionality principle reads: '[T]he action of the EU must be limited to what is necessary to achieve the objectives of the Treaties. In other words, the content and form of the action must be in keeping with the aim pursued'.[77] Proportionality is one of the underpinning principles of how European Union exercises its powers. 'Risk-based approach' is the synonym of this definition. In the context of AI regulations proportionality means application and enforcement of regulations in such a way that takes into account the applicability of a specific regulation to the unique circumstances (eg size, structure, type of services provided, operational set-up, market impacts) of a particular regulated firm.

A risk-based approach is widely regarded as the best approach to regulating emerging technologies due to its flexibility. It is explicitly referenced throughout the proposed EU AI Act (Article 2.3 of the Explanatory Memorandum) and applies across all of EU hard and soft laws by default, even when it is not explicitly referenced.

---

[75] BaFin, note 15 above.

[76] We wanted to avoid 'over-implying' and consequently we only counted the three regulations (MIFID II, IOSCO, BaFin) where algorithm inventory was alluded to in the relatively strongest way.

[77] See EurLex, 'Principle of Proportionality', https://eur-lex.europa.eu/EN/legal-content/glossary/proportionality-principle.html.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

Outside of the EU, IOSCO, ICO, PDPC, and HKMA also refer to it. One could argue that even when it is not explicitly mentioned, it is reasonable to expect a risk-based approach by default in most jurisdictions.

E. Business/Conduct

1. Internal skills

Internal skills and competence are the top operational consideration by popularity. They are prominently mentioned by RTS 6, IOSCO, ICO, HKMA, and FSB. The proposed EU AI Act mentions skills as well, though in the context of skills within the regulatory agencies, and not in the AI industry per se (FSB raises a similar point).

There is little variation among regulators and publications. RTS 6 and IOSCO cover it most comprehensively; they are also unique in explicitly referencing the importance of skills within the compliance function. RTS 6 mandates that the compliance function should be knowledgeable enough to be able to challenge the trading teams (although it is slightly inconsistent, requiring in Article 2 'at least a general understanding', but requiring 'sufficient knowledge' in Article 3); IOSCO makes an identical recommendation. IOSCO also lists skills as one of the potential mitigants to the risks posed by the use of AI (other mitigants being culture, accountability, and operational resilience).

2. Senior management accountability

Management accountability is closely linked to skills. The message is universal across all regulations: there need to be clear, unambiguous lines of accountability of human senior management, with no function left in a 'blind spot'. The key regulation in this area is SM&CR. SM&CR is in part neutral with respect to business areas, as it imposes an accountability regime on all senior managers; on the other hand, it specifically lists algorithmic trading as one of its 'certification functions'. Certification functions are not part of senior management but can have a significant impact on customers and the market, and firms need to certify the suitability of employees in these functions at least once a year. ICO guidance overlaps with SM&CR in reiterating senior management's responsibilities, thus making the UK probably the strictest jurisdiction as regards accountability.

IOSCO[78] recommends designating a senior manager in charge of AI deployment, as well as on the compliance side. BaFin[79] explicitly reiterates the responsibility of senior management, even in case of automated decision-making; HKMA[80] makes an identical point.

[78] IOSCO, note 14 above.

[79] BaFin, note 15 above.

[80] HKMA, 'High-Level Principles on Artificial Intelligence', 2019.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

3. *Market abuse*

Market abuse is defined and addressed in existing regulations, such as the EU's Market Abuse Regulation ('MAR'[81]). It can be broadly defined as activities in which party or parties artificially impact the prices at which securities are trading or through their knowledge of non-public material information profit from transactions in financial markets to the detriment of other market participants. The issue of accountability for market abuse is addressed in a similar fashion across many jurisdictions: there are regulatory sanctions (sometimes referred to as administrative) such as professional bans and substantial monetary fines in addition to forgoing all illegal gains. The sanctions can be levelled against both natural and legal persons (financial firms).

Interestingly, regulations can be ambiguous as regards the intentionality of market abuse (eg MAR focuses on market abuse actions and does not explicitly state that they have to be intentional). MAR's companion law, the Market Abuse Directive ('MAD'[82]) proposes that serious cases of market abuse should be criminalised when committed with intent.[83] Intentionality is very important, because AI and algorithms cannot have their own intentions—they either transmit and execute the intentions of their human operator or learn illegal practices by themselves.[84] There is an expectation that financial firms are sufficiently prudent to render inadvertent and learned market abuse impossible. This is stated, for example, by RTS 6, IOSCO,[85] or FSB.[86]

It appears that regardless of the situation (executing the intentions of a human operator or self-learned behaviour) existing market abuse regulations provide sufficient provisions for potential abuses committed by AIs by having a broad spectrum of administrative, monetary, and criminal penalties at their disposal. One challenging aspect could be the apportioning of accountability between relevant senior managers and the firm as a whole. In our view, as long as the senior managers' intent to commit market abuse is not proven then it is likely that they could be subject to administrative sanctions, while monetary fines would likely be borne by the firm.

4. *Suitability*

MIFID II includes detailed and explicit provisions on suitability of financial products vis-à-vis client's financial knowledge and their risk tolerance. Suitability is not

---

[81] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on Market Abuse (Market Abuse Regulation), 2014.

[82] Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on Criminal Sanctions for Market Abuse (Market Abuse Directive), 2014.

[83] In the UK, insider trading is a criminal offence under Article 52 of the Criminal Justice Act 1993.

[84] M P Wellman and U Rajan, 'Ethical Issues for Autonomous Trading Agents' (2017) 27 *Minds and Machines* 609; R Cooper, M Davis, and B Van Vliet, 'The Mysterious Ethics of High-Frequency Trading' (2016) 26(1) *Business Ethics Quarterly* 1.

[85] IOSCO, note 14 above.

[86] Financial Stability Board, note 9 above.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

related to AI, algorithms or any other technology—it is a universal consideration. Article 24(2) MIFID II requires the investment firms to 'understand the financial instruments they offer or recommend'.[87] Despite its brevity, this provision has substantial bearing on how AI can be used in the investment decision-making process. An investment-picking AI not being fully transparent and explainable would violate that requirement.

Article 25 MIFID II is very clear as regards the requirements of suitability. When the investment recommendation is made by a human (MIFID II refers to humans as 'natural persons') errors are possible (eg recommending a very long-term strategy to an investor in their 80s), but a specific recommendation can always be questioned and explained (Point 82 of the MIFID II preamble mandates the investment advisor to provide a written statement on 'how the advice given meets the preferences, needs and other characteristics of the retail client'). An AI investment-picker needs to be able to do the same. A 'black box' approach is not acceptable.

IV. CONCLUSION

There is a common belief in the investment management industry that its use of AI is yet to be regulated. Our analysis proves that the regulatory landscape for AI relevant to investment management is far from empty. Some of the existing regulations may be 'hiding in plain sight', while the many soft laws proposed worldwide may be better known in their local markets than internationally.

This Article has identified seventeen regulatory themes from an interdisciplinary, interlocking framework of regulating AI in the investment industry. This framework is unique in multiple ways.

First, the very concept of regulating a specific technology runs counter to the default approach of technological neutrality. AI is neither first nor unique in that respect. The cloud was the first technology with a dedicated set of regulation in financial services, but AI regulations go deeper than cloud regulations in covering considerations such as specific use cases, ethics, or societal impacts—while remaining neutral with respect to specific AI techniques.

Second, the importance of interdisciplinarity cannot be overstated. The mosaic of connections and dependencies created by AI will likely force a radical change—both cultural and operational—in governance and oversight. Business models will need to change from the traditional top-down approach to a largely flat-structured cluster of interdisciplinary stakeholders, breaking down traditional organisational 'silos'. However, that change must go hand in hand with unambiguous delineation and attribution of individual accountability of each stakeholder. Another aspect of interdisciplinarity is the opportunity it provides for academia,[88] the industry, industry bodies, and regulators to collaborate. Some of those players have successfully collaborated

[87] See note 44 above.

[88] Cf Section 4.3 of our previous research (W Buczynski, F Cuzzolin, and B Sahakian, 'A Review of Machine Learning Experiments in Equity Investment Decision Making: Why Most Published Research Findings Do Not Live Up to Their Promise in Real Life' (2021) 11 *International Journal of Data*

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

for years, but academia's relationship with the financial industry has been more complicated. Academic research (with the exception of seminal concepts such as Markowitz's risk/return framework,[89] Fischer Black and Myron Scholes's option pricing model,[90] or Eugene Fama and Kenneth French's three-factor model[91]) is not often utilised in investment management, and some practitioners believe that it is of little practical value in the 'noisy' real-world setting. However, AI is beyond a doubt driven by academic research, and academia offers a lot of valuable insights on the use of AI in the investment industry—to do so, however, it must become a part of the conversation. Innovative public/private partnerships may be the way to bring these stakeholders together. One such partnership, the AI Private/Public Forum ('AIPPF') has recently been trialled in the UK. Set up jointly by the FCA and the Bank of England, it included stakeholders from different areas of financial services as well as academia, with regulators driving the agenda. The AIPPF could become a blueprint for similar AI partnerships worldwide.

Compliance and governance of AI are also very important. The compliance function (a team responsible for a financial firm's adherence to laws and regulations as well as ethical and professional standards[92]) needs to be involved in the deployment of AI from the planning phase, through implementation, all the way to ongoing post-deployment oversight. That is a huge change—culturally and organisationally—from the way the compliance function has traditionally been involved in technology oversight (which often meant not at all). Compliance (and broader General Counsel) have historically been focused on issues which had no relation to technology (eg anti-money laundering, conflicts of interest, market abuse). AI (and the cloud before it) mark a disruptive change for compliance, which will require new skills and new, interdisciplinary collaborations.

AI's impacts (actual, potential, and unforeseeable) are likely to fit the criteria of the precautionary principle. Its genesis is in environmental law,[93] but has since been generalised as an 'approach in policy making that legitimizes the adoption of preventative measures to address potential risks to the public or environment associated with certain activities or policies'.[94] The principle is one of the pillars of EU decision-

---

(F'note continued)

Science and Analytics 221, https://rdcu.be/ch7Xo) where we first highlighted the importance of an interdisciplinary approach.

[89] H Markowitz, 'Portfolio Selection' (1952) 7(1) *The Journal of Finance* 77.

[90] F Black and M Scholes, 'The Pricing of Options and Corporate Liabilities' (1973) 81(3) *The Journal of Political Economy* 637.

[91] E F Fama and K R French, 'Common Risk Factors in the Returns on Stocks and Bonds' (1993) 33(1) *Journal of Financial Economics* 3.

[92] See Robert Walters, 'The Role of Compliance Officer', https://www.robertwalters.us/blog/the-role-of-a-compliance-officer.html.

[93] The early definition dates back to the environmental summit in Rio in 1992 and reads: 'Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation'.

[94] Encyclopaedia Britannica, 'Precautionary Principle', https://www.britannica.com/topic/precautionary-principle.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

making process under uncertainty. Interestingly, the discussion of the precautionary principle is missing in EU regulations. It can either be an oversight or the regulators consider the precautionary principle to be so fundamental that it does not need to be explicitly mentioned. Regulators will need to carefully weigh these considerations and balance them in ways that protect the market and the consumers, whilst also allowing technology to develop and move forward. A proactive (innovative) approach protects the regulators from being surprised by innovations, but risks becoming seen as prescriptive, which is counter to the regulators' technology-neutral mandate. A reactive (cautionary) approach is less invasive but risks that the industry and its interests take the lead in the regulatory discourse. The former approach risks stifling innovation (if a technology becomes over-regulated), while the latter risks enabling a regulatory gap—a situation where a technology surpasses the ability of law to govern it.[95]

Systemic risks have been discussed under the complexity theme. The default perspective of most (if not all) relevant laws is the individual company level, with systemic risks being either an afterthought or a non-consideration. We would like to suggest that systemic risks should feature much more explicitly and prominently in future AI regulations. By contrast, the importance of transparency and explainability have been very clear (and uncontested) from day one. The lesser-appreciated consideration is that, at present, regulatory provisions regarding transparency and explainability—if taken literally—might be challenging to implement on a technical level. The issue is that some of the cutting-edge AI techniques such as deep learning use highly non-linear functions, which makes their outcomes challenging to explain and interpret. Fortunately, there are approximations which can provide partial explanations, eg determining the ten features that influenced the outcome the most. Deep learning algorithms can sometimes be approximated by interpretable models (eg decision trees or random forests) and interpreted via this proxy.[96] They can even be replaced by the simpler, interpretable models altogether (as proposed by BaFin or the ICO). There is also ongoing work to make deep learning algorithms more explainable without sacrificing their performance.[97] There needs to be an open dialogue and a delicate balance between best efforts (on the part of the regulated firms) and enforcement (on the part of regulators).

A unique challenge facing AI regulation is that due to it being completely novel, there is no way of knowing whether the actual outcomes will be the same as the intended outcomes. This may complicate the regulators' incentives in drafting and passing AI regulations, because there is little first-mover advantage (other than political—setting the tone of the debate, creating a reference for all future regulations

[95] C I Gutierrez, 'Can Existing Laws Cope with the AI Revolution?', *Brookings*, 8 July 2020, https://www.brookings.edu/techstream/can-existing-laws-cope-with-the-ai-revolution.

[96] C Beisbart and T Raz, 'Philosophy of Science at Sea: Clarifying the Interpretability of Machine Learning' (2022) 17(6) *Philosophy Compass* e12830.

[97] Eg DARPA's (Defense Advanced Research Projects Agency) Explainable Artificial AI (XAI) Programme, https://www.darpa.mil/program/explainable-artificial-intelligence.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

etc)—if anything, there is first-mover *dis*-advantage because whichever regulations are enacted first, they may be imperfect and controversial.

As is the case with any regulation, questions may be raised as to what its objectives should be, and how its quality should be measured. The objectives are clear: market stability; investor protection; lowering of costs; and better products—standard tenets of financial regulation.[98] Regulation should also align with and drive values such as being beneficial, non-discriminatory, transparent, fair, and inclusive.

Another relevant question for financial regulators to consider is aligning financial AI regulations with broader (national or regional) AI strategies[99] as well as applicable strategy-adjacent instruments.[100] Alignment along the lines of values is a realistic scenario. It would ensure that AI observes the same fundamental principles (eg governance—one of the pillars of the UK AI strategy) across different industries whilst allowing the regulators to set detailed laws in accordance with the specific nature of their regulated industries.

It is important to consider what the interplay between AI regulations and AI ethical standards should be considering the substantive volume of research on AI ethics that has been produced worldwide in recent years.[101] We see ethics and regulations as complementing each other: regulations mandate appropriate business conduct, controls and governance, while ethics point financial organisations towards the values and outcomes that benefit not just the organisations, but also their clients and society at large.

Lastly, there is also a fundamental question of what the clients want. Do they feel comfortable with AI and algorithms managing their investments? In our view, the clients' implicit consent should not be taken for granted. The industry should proactively consider consumer sentiments in its AI strategy and governance, for example by emphasising the humans' role as primary decisionmakers.

The regulatory landscape for AI in investment management may be far from empty, but AI's 'regulatory journey' is only just beginning. The interpretation of

---

[98] Cf FCA's Mission Statement, https://www.fca.org.uk/publication/corporate/our-mission-2017.pdf.

[99] Eg UK's National AI Strategy, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf.

[100] Eg the policy paper 'The Kalifa Review of UK FinTech' in the UK (https://www.gov.uk/government/publications/the-kalifa-review-of-uk-fintech), which explicitly recommends to 'consider the regulatory implications of AI'.

[101] Those include publications from government and public agencies (eg European Commission's 'Ethics Guidelines for Trustworthy AI'), academic and international organisations (eg Université de Montréal: 'Montréal Declaration: Responsible AI'; The Royal Society: 'Machine Learning: The Power and Promise of Computers that Learn by Example'; Future of Life Institute: 'Asilomar AI Principles'), and the industry (eg IBM, Google/DeepMind, Microsoft, Intel, Accenture, Sony). There is also a smaller subset of research focused specifically on AI ethics in financial services, eg D Mhlanga, 'Industry 4.0 in Finance: The Impact of Artificial Intelligence (AI) on Digital Financial Inclusion' (2020 8(3) *International Journal of Financial Studies*; E Svetlova, 'AI Ethics and Systemic Risks in Finance', *AI and Ethics*, 2022; E Kurshan, J Chen, V Storchan, and H Shen, 'On the Current and Emerging Challenges of Developing Fair and Ethical AI Solutions in Financial Services', 2 November 2021.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

the laws may be just as important as the laws themselves and will likely require an ongoing dialogue between the industry and the regulators. New developments will bring new applications as well as challenges, which will in turn place new demands on regulation. In our view AI regulation will continue to develop in lockstep with the technology for years to come.

Appendix 1 – Collation of Relevant Regulations

Our primary jurisdictions of reference are the United Kingdom and the European Union. Reference materials are taken either directly from financial regulators or from established industry groups and bodies. We approached them in a systematic review fashion, although traditional article database screening (eg Google Scholar or Cambridge University's iDiscover) did not apply. Instead, a two-step regulatory horizon scanning was conducted:

1. Jurisdictions of interest were identified (UK, EU[102]—which were our primary interest; UAE, Hong Kong, Singapore, China, Taiwan, South Korea, Japan, Australia—which were our secondary interest). United States, due to a multitude of regulators and agencies (SEC, CFTC, the Fed, FTC, to name a few) warrants a standalone, separate article.
2. Hard and soft laws applicable to selected territories from the AI and/or algorithm perspective were researched and included in the Article. Some jurisdictions turned out not to have applicable regulations at the time of writing (Taiwan, Australia) or did not have quality English translations available (South Korea[103]).

Appendix 2 – List of Source Regulations and Applicable Jurisdictions:

1. General Data Protection Regulation (GDPR) (EU).
2. Markets in Financial Instruments Directive II (MIFID II) (EU). Regulatory Technical Standard 6 (RTS 6).
3. Senior Managers & Certification Regime (UK).
4. The proposed EU AI Act (EU).

[102] EU regulatory horizon scanning consisted of two steps. In the first step, EU-wide regulations, such as MIFID II, were identified, and in the second step, applicable additional regulations on individual member state level were identified.

[103] On 8 July 2021, South Korea's Financial Services Commission issued guidelines on AI in financial services. The summary press release was published in English (https://www.fsc.go.kr/eng/pr010101/76209), but the guidelines themselves were not. Unfortunately, we were unable to include them in our analysis due to the lack of an English version.

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press

5. IOSCO, 'The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers' (international).
6. 'Liability for Artificial Intelligence and Other Emerging Digital Technologies' (EU).
7. 'White Paper on Artificial Intelligence—A European Approach to Excellence and Trust (EU).
8. 'Report on Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics' (EU).
9. BaFin, 'Big Data Meets Artificial Intelligence – Results of the Consultation on Bafin's Report' (Germany).
10. ICO, 'Guidance on the AI Auditing Framework Draft Guidance for Consultation' (UK).
11. ICO, 'Explaining Decisions Made with AI' (UK).
12. PDPC, 'Model Artificial Intelligence Governance Framework (2nd Edition)' (Singapore).
13. Guiding Opinions of the PBOC, the China Banking and Insurance Regulatory Commission, the China Securities Regulatory Commission, and the State Administration of Foreign Exchange on regulating the asset management business of financial institutions (China).
14. HKMA, 'High-Level Principles on Artificial Intelligence' (Hong Kong).
15. METI, 'Governance Guidelines for Implementation of AI Principles Version 1.0' (Japan).
16. OECD, 'Artificial Intelligence, Machine Learning and Big Data in Finance' (international).
17. FSB, 'Artificial Intelligence and Machine Learning in Financial Services' (international).

https://doi.org/10.1017/cel.2022.10 Published online by Cambridge University Press