MANCHESTER 1824

The University of Manchester

Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry

Free paper

By Dr. Joseph Lee, Senior Lecturer

www.manchester.ac.uk/techlaw

Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry

Joseph Lee©, Senior lecturer in law, University of Exeter, UK
j.lee@exeter.ac.uk

Abstract

This paper discusses the design of the legal and regulatory framework for using artificial intelligence (AI) in financial services markets to enhance access to finance (financial inclusion). The author argues that the development of AI should continue to adhere to the regulatory objectives of market safety, consumer protection, and market integrity. However, to ensure equality and fairness, access to finance should be made a clear policy choice. In Part I, the author discusses how AI can lead to systemic risks and market manipulation on trading platforms. For example, by examining the use of algorithms for trading on the capital market, the author discerns the regulatory objectives and the possible methods of regulation for peer-to-peer platforms. In Part II, the author discusses how the use of AI to provide consumers with investment advice, such as financial advice provided from robo-advisers, can close the investment advise gap and provide consumers access to finance. The current regime does not provide adequate protection to financial consumers in this regard. In Part III, the author discusses how AI can be used as a form of RegTech to streamline compliance processes, thereby increasing competition in financial markets and providing a benefit to consumers. However, this use may be in conflict with privacy, data protection, and ethical concerns. The author makes policy recommendations and suggests some directions for governance in the use of AI in financial services to enhance access to finance. The findings of this paper are relevant to research on the future governance of artificial intelligence in financial services, public policy innovation, and urban development.

Keywords AI, financial services, access to finance, investor protection, GDPR, privacy rights

Introduction

1. Access to finance

AI is seen as a threat to employment, as it will take away manual jobs.[1] This threat is also true for financial services.[2] Nutmeg Review in 2017 revealed that a large proportion of the traditional business of financial advisers is threatened by automated services.[3] Despite this, the uncertainty that AI brings to incumbent operators, consumers, and financial regulators has not stopped investment in AI FinTech. To strengthen its legitimacy in the financial services sector and to gain public acceptance, AI must provide some social benefits. Therefore, access to finance,[4] also referred to as financial inclusion, should be set as the policy priority in the regulation of the design, development, and deployment (DDD) of AI.

According to the definition given by the Financial Inclusion Report 2018/19, "financial inclusion means that individuals, regardless of their background or income, have access to useful and affordable financial products and services. This includes products and services, as well as transactions and payment systems, and the use of financial technology."[5] The provision of access to finance should aim to enable those currently excluded by the existing systems to participate in the financial markets. To benefit from the economic growth, these individuals should have access to capital pools for personal or business finance, access to real-time information with the aid of data analytics, and have access to a range of investment providers. In this article, the author will focus on three aspects of how AI can enhance financial inclusion: 1) increasing participation in peer-to-peer platforms by providing security to them, 2) closing the advice gap in investment services; and 3) allowing more financial outlets to be operated in the financial services sector by reducing their operational costs, such as compliance costs.

---

[1] BBC News, https://www.bbc.co.uk/news/business-45240758 (last accessed on 25 November 2019).
[2] Marria V, https://www.forbes.com/sites/vishalmarria/2018/09/26/is-artificial-intelligence-replacing-jobs-in-banking/#2b0d81343c55 (last accessed on 25 November 2019).
[3] Meola A, https://www.businessinsider.com/nutmeg-review?r=US&IR=T (last accessed on 25 November 2019).
[4] Report of the Business, Energy and Industrial Strategy Committee of 2016/17 on Access to Finance.
[5] Report of HM Treasury and of Department for Work and Pensions of 2018/19 on Financial Inclusion.

The paper will discuss the regulatory objectives and methods of regulation in these three areas by looking at close parallels. The first is the use of AI in the trading platforms for capital optimisation, such as increase of efficiency, accuracy, and speed of capital optimisation through the foundations of computing capabilities, big data and mathematical concepts built by AI and Machine Learning.[6] The second is the use of robo-advisers to provide investment services, such as identifying wider sources of available funds for FinTech lending to SMEs and clients through AI and ML's advanced credit scoring.[7] And the third is the use of AI in RegTech services to streamline compliance costs,[8] such as the costs involved in the Know Your Consumer processes ('KYC'). In this way, the author will examine how AI-facilitated access to finance can align with current regulatory objectives and methods of regulation. Whether the provision of this access will conflict with other values, such as privacy, data protection, and ethics will also be examined.

Part I

1. Algorithmic trading on regulated platforms

The UK authorities regard financial technology as an efficient tool to tackle financial exclusion and also a way to encourage firms to develop innovative processes and thus increase consumer access to the financial services.[9] Peer-to-peer platforms have been regarded as providing a more economic way to bring businesses and investors together. Compared with bank saving, peer-to-peer (p2p) platforms offer higher interest rates.[10] In addition, investments through p2p platforms offer higher liquidity than traditional property investments.[11] Most importantly, p2p platforms normally split capital into several parts for multiple borrowers, thus lowering the risk of occurring major losses. Algorithmic trading can be used in p2p platforms to increase access to finance, particularly in capital allocation. Tightening of bank lending policies followed the financial crisis, p2p lending has become a major player in global financial markets. For instance, LendingClub Inc. developed its own platform, relying on sophisticated algorithms to pair borrowers and investors and also to evaluate the attributes of both sides.[12]

Not only on the p2p lending platforms, it is envisaged that algorithms may also be used for secondary securities trading on blockchain-based trading platforms such as ICOs. For instance, in early 2019 the London Stock Exchange invested 20 million dollars to Nivaura, a blockchain start-up that specialises in fully-automated tokenised bonds recorded on a blockchain.[13] In April 2019, LSE and Nivaura issued shares with £ 3 million on LSE'S test network.[14] While traders in the financial markets are using algorithms to make gains, the author argues that similar tools and opportunities should also be given to investors and consumers. This is a way to provide access to financial markets. Therefore, algorithms should be made available through market competition. Real-time data should also be made available to consumers and investors, rather than being an expensive commodity only available to those who can afford it.

However, users need to feel confident that the platforms on which algorithms are used are not likely to cause a market crash or to manipulate the market. Market crashes due to human behaviour have occurred in modern capital markets[15] such as the 'Dotcom Bubble Burst' in the 1990s and the 1998 'Asian Crash'. AI does not reduce the risk of a market crash and may even increase the chances of it happening.[16] This can be seen in the market crash in 2008 for which High Frequency Trading (HFT) has been considered the cause, or at least a contributing factor.[17]

---

[6] FSB (2017).
[7] *Ibid*, p 2.
[8] Dunnly, https://dunnly.com/learn-how-banks-and-finance-houses-use-ai-for-regulatory-compliance/ (last accessed on 25 November 2019).
[9] See *infra* n 5.
[10] Bankrate, https://www.bankrate.com/uk/savings-accounts/peer-to-peer-savings/ (last accessed on 25 November 2019).
[11] Mortgage Introducer, https://www.mortgageintroducer.com/p2p-lending-offers-attractive-entry-point-property-investment/ (last accessed on 25 November 2019).
[12] Mark Albertson, https://siliconangle.com/2018/08/24/%E2%80%8Bthe-sophisticated-algorithms-behind-peer-peer-money-lending-guestoftheweek/ (last accessed on 25 November 2019).
[13] The Trade, https://www.thetradenews.com/lseg-leads-20-million-funding-round-blockchain-startup/ (last accessed on 25 November 2019).
[14] The Telegraph, https://www.telegraph.co.uk/technology/2019/04/15/london-stock-exchange-accepts-first-listing-blockchain-token/ (last accessed on 25 November 2019).
[15] Jhun et al. (2018), pp 4477, 4505.
[16] Bank of England and FCA (2019).
[17] Sornette and Becke (2011).

Hence, the regulation of HFT can provide a blueprint for regulating algorithmic trading on a peer-to-peer platform.[18]

HFT is a type of algorithmic trading that has been used for more than a decade on trading platforms.[19] The reason for its emergence was the market liberalisation and market competition that substantially reduced the trading revenues of the trading platforms.[20] HFT allows trading venues to raise trading fees. It is not yet clear if HFT will be used in other trading platforms, such as p2p platforms,[21] to provide the same benefit. The business model on p2p trading platforms may not be the same as that on securities trading platforms. Technical obstacles may need to be overcome; for instance, the speed on a blockchain-based p2p platform may not be sufficient to support HFT.[22] However, the lessons learned regarding the risks in algorithmic trading provide a good regulatory framework that can be applied to provide security for users on the platform.[23]

HFT, computerised trading controlled by algorithms, is a subset of the broader (and older) phenomenon of algorithmic trading.[24] In essence, algorithmic trading is simply the use of specialised software to implement pre-determined decision-making rules for the evaluation of market conditions and other data in order to make trading decisions without human involvement.[25] Hence, in algorithmic trading, the traders' computers directly interface with trading platforms, placing orders without immediate human intervention. The computers observe at very high frequency market data and possibly other information. Based on a built-in algorithm, trading instructions are sent to the platform, often within milliseconds. A variety of algorithms are used for identifying arbitrage opportunities; for seeking the optimal execution of large orders at a minimum cost; and for seeking to implement longer-term trading strategies.[26]

2. Market safety regulation

The main focus of regulation on algorithmic trading is market safety to address systemic risks caused by algorithmic trading. These include flash crashes, reduced liquidity, and herding behaviour.[27]

2.1 Flash crash

A market crash, predating the involvement of AI, has happened in the capital markets and the regulations put in place to avoid a recurrence focuses primarily on human conduct. When machines are involved, systemic risk becomes the main concern, so market safety regulation needs to be introduced to provide security. The EU and UK regulators have introduced measures to mitigate the risk of a flash crash caused by AI. Algorithmic trading can result in a 'flash crash', for example, when the withdrawal of stock orders rapidly amplifies price declines.[28] After the flash crash in 2010,[29] the UK's Financial Conduct Authority, alongside the Prudential Regulation Authority, started closely monitoring HFT. HFT firms were considered to have contributed to market instability and to the overall lack of investors' trust in the market.[30] In the same effort, the EU regulates HFT activities under the 'Markets in Financial Instruments Directive II' and the 'Markets in Financial Instruments Regulation', known together as 'MiFID II and MiFIR'.[31] MiFID II has three main strands. First, it provides for a new operational

[18] Morelli (2017), pp 201, 229.
[19] Woodward (2017), pp 2, 44.
[20] Breckenfelder (2019).
[21] citanic and Kirilenko, https://www.ft.com/content/0f18ea78-293f-11e8-b27e-cc62a39d57a0 (last accessed on 25 November 2019).
[22] Andoni et al. (2019), pp 143, 174.
[23] Barrales (2012), pp 1195, 1262; also see McNamara (2016) pp 71, 150.
[24] UK Government's Foresight Project of 2012 on High Frequency Trading – Assessing the Impact on Market Efficiency and Integrity.
[25] See https://pdfs.semanticscholar.org/711e/f95dfa873e06274df93fd12c2b766078a837.pdf (last accessed on 25 November 2019).
[26] Dignum(2019) pp 130,136.
[27] Turner (2019); also see O'Mahony https://www.irishtimes.com/business/personal-finance/could-high-frequency-traders-cause-another-flash-crash-1.2233576 (last accessed on 25 November 2019).
[28] Mack (2016), p 92; also see Fitsills (2019), p 4.
[29] Trotman https://www.telegraph.co.uk/finance/financial-crime/11553696/What-happened-during-the-Flash-Crash.html (last accessed on 25 November 2019).
[30] See *infra* n. 23, p 1197.
[31] Busch (2016), pp 72, 82.

regime governing algorithmic trading by investment firms.[32] Second, it extends its scope to encompass all firms engaging in algorithmic trading, in particular, specialist firms that undertake HFT.[33] Third, it imposes operational requirements on trading venues, such as exchanges e.g. platforms. [34] For instance, circuit breakers, also called shock absorbers, are required for trading venues such as exchanges to temporarily halt trading when market prices as indicated by a benchmark index fall by a certain percentage during a specific period.[35]

Under the first strand, investment firms that engage in algorithmic trading are subject to a 'targeted operational regime'.[36] They are required to have in place effective systems and risk controls to ensure that trading systems are resilient and maintain the appropriate thresholds and limits to prevent incorrect or erroneous orders which may create or contribute to a disorderly market.[37] In the UK, these algorithmic trading requirements were implemented through Chapter 7A of the Market Conduct Sourcebook.[38] The second strand requires that firms must have 'effective business continuity arrangements' to handle any trading system failure and must ensure that systems are fully tested and continuously monitored.[39] Third, HFT firms must have an emergency 'kill functionality', which allows them to cancel all unexecuted orders with immediate effect.[40]

In addition to this organisational requirement, all firms must notify the Financial Conduct Authority and the venue's competent authority if the firms engage in any HFT on any EU trading venue.[41] Lastly, firms must carry out an annual self-assessment and issue a validation report covering such elements as governance, control framework, and overall compliance with the other MiFID II requirements.[42] Firms are required to identify the algorithm ownership, establish testing processes, and identify relevant environmental factors, such as the counterparties that use algo-trade.[43] They are also required to identify risks and provide risk mitigation measures.

The Prudential Regulatory Authority has also published a consultation paper to accompany these current regulations which focuses on the proposed expectations of a firm's policies for the 'governance and risk management of algorithmic trading'.[44] Some countries go further than the EU regulations and have adopted measures such as a requirement to hold a licence to operate HFT. In Germany, under s.32 of the German Banking Act, HFT firms need to hold a licence issued by the German Federal Financial Supervisory Authority.[45]

2.2 Liquidity risk and Procyclical behaviour

To address liquidity risk, HFTs are required to register as market makers.[46] A market maker is a market participant that buys and sells large amounts of a particular asset in order to facilitate liquidity and ensure the smooth running of financial markets.[47] Market makers are obliged to continually quote bid and offer prices, and to guarantee the full sale or absorption of the security at a certain price.[48] When the market becomes stressed,[49] an HFT has an

[32] Moloney (2016), p 528.
[33] Banks and Pool (2018).
[34] *Ibid*.
[35] Definition given by Financial Times Lexicon.
[36] Moloney (2014), p 529.
[37] Article 17 of MIFID II; *Ibid*.
[38] See https://www.fca.org.uk/publication/multi-firm-reviews/algorithmic-trading-compliance-wholesale-markets.pdf (last accessed on 25 November 2019).
[39] *Ibid*, p 5.
[40] FCA, https://www.fca.org.uk/publication/multi-firm-reviews/algorithmic-trading-compliance-wholesale-markets.pdf (last accessed on 25 November 2019).
[41] Section 17 (2), MiFID II.
[42] See *infra* n. 40.
[43] Supervisory Statement ss5/18 of Bank of England, Supervisory Statement, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2018/ss518, also see Policy Statement of FCA on Algorithmic and High Frequency Trading Requirements, https://www.fca.org.uk/mifid-ii/8-algorithmic-and-high-frequency-trading-hft-requirements (last accessed on 25 November 2019).
[44] Report of FCA on the Supervision of Algorithmic Trading, https://www.fca.org.uk/news/press-releases/fca-publishes-report-supervision-algorithmic-trading.
[45] *Ibid*, P 245.
[46] See *infra* n. 43.
[47] Shen and Starr (2002) pp. 53, 58.
[48] Benos and Wetherilt (2014).
[49] Scharpiro (2018); also see Seidel (2011) pp 118, 120.

additional duty to ensure liquidity. Market makers have to protect proposals to purchase and sell stocks at levels corresponding to different price and size thresholds. Market makers have to comply with four different elements: to offer the quote at the best price in a specified period of time; to offer the quote at prices within the specified period of time from the National Best Bid or Proposal; to quote with a minimum dimension and various prices; and to build markets for a minimum amount of stocks.[50] Market makers take the highest trading risk to comply with the four elements, and are therefore required to maintain the necessary amount of capital.[51] Additionally, if market prices escalate or decrease more than a certain amount, exchanges have the authority to limit the usage of specific trading tactics.[52]

There is also a risk of procyclical behaviour when market participants begin to use similar AI and machine learning programmes.[53] The consequent correlated risks may entail financial stability risks.[54] If a machine learning-based trader outperforms others, this could in the future result in many more traders adopting similar machine learning strategies, even if this reduces the profitability of such strategies.[55] While there is no evidence to date of this having occurred, it could become relevant as such trading strategies are increasingly adopted. As with any herding behaviour in the market, this has the potential to amplify financial shocks. The main risk is the creation of procyclical behaviour that is harmful to financial stability.[56] If regulators develop a preference for a robo-adviser design that is understood by firms, it could result in a convergence of models that would increase the probability of a systemic crisis.[57]

2.3 Same approach to peer-to-peer trading platforms

Market safety and soundness regulations are aimed at providing financial stability and security to the users. In this section, the author uses the example of HFT to identify some of the risks to market stability of using AI. The main approaches to regulating activities and risks are internal systems and controls, self-assessment, and the reporting by both firms and trading venues.[58] There are also specific requirements to deal with market crashes, liquidity risk, and correlated losses. In addition, traders using AI will need to fulfil their duties as market makers. To avoid similar losses, brokers and investor advisers using similar AI technology will need to be subject to the same systems and controls as those used for HFT.

In the application of regulations for the use of AI on p2p trading platforms, market safety and market integrity, alongside the access to finance, should continue to be the regulatory objectives. The risks, such as systemic risk, liquidity risk, and correlated risk, are the same as those on the capital market trading platforms. The difference lies in the methods of regulation. On the p2p platforms, organisational regulation is unlikely to be implemented for individual participants on the platforms. The regulatory emphasis will be more on requiring the trading platforms to vet individuals who use algorithms to make transactions, to maintain the capacity to absorb the liquidity risk, and to have surveillance to control market manipulation. In fulfilling the objective of providing access to finance, the cost of maintaining the system should not be transferred to the users. If the cost of addressing these risks is too high, fewer platforms will be willing to operate. Hence, there should be ways to implement the systems of risks and control (organisational requirement) in a more economical way, such as by using certification systems to allow algorithmic uses on the platforms (an alternative way to submitting source code) and using RegTech solutions to monitor market manipulation.[59] In addition, the regulators can regulate the financial instruments (through product intervention power[60]) that could be used on the trading platforms.

[50] See *infra* n. 23, p 1246
[51] *Ibid*., p 1248
[52] *Ibid*., p 1247
[53] Danielsson et al. (2017).
[54] *Ibid.*
[55] Shabbir and Anwer (2018) pp. 893, 897.
[56] Papaioannou et al. (2013).
[57] Baker and Dellaert (2018), p 746
[58] See *infra* n. 31, pp 72, 82.
[59] See 2.1, Technical methods in EU Ethics Guidelines for Trustworthy AI; also see Report of Session 2017-19 of Science and Technology Committee, House of Commons (2018) on Algorithms in Decision-Making.
[60] S 137D, FSMA 2000.

Part II Investor protection

AI should give more freedom of choice as well as security to investors. It can enable access to finance by providing more economical investment advice to consumers who are excluded from accessing investment opportunities through lack of information. This presents an opportunity for the use of AI to provide services to consumers for both execution or investment advice through, for example, robo-advisers.[61]

When AI is consumer facing, such as in the use of robo-advisers or the use of AI by intermediaries for stock and fund selections, the focus of regulation is on both the ex ante (including reviewing the algorithmic models, CDD and algorithm explication[62]) and the ex post protection of investors (compensation and liability for AI[63]), especially retail investors. Hence, the main issues are the consumers' understanding of the nature of AI (through algorithm explicability[64]), the risk of using AI, and the liability associated with AI. Investors should also be protected in a fiduciary context: the providers of AI services have an obligation to act in the best interest of the customers and to present no conflict of interest.[65]

1. Using robo-advisers to close the investment advice gap

There is no consensus on the definition of the financial advice gap.[66] According to the definition given by the Financial Advice Market Review (FAMR), the financial advice gap refers to "situations in which consumers are unable to get advice and guidance on a need they have at a price they are willing to pay".[67] Cost is not the only factor causing this gap, and the financial advice gap should be defined as "the difference between the number of people who currently seek advice, and those who would seek advice if a cheaper and less intensive process existed".[68] However, there is a common view that a gap exists for (potential) customers who have lower incomes or lower level of assets and could either not afford the advisory fee or find it hard to access.[69] The conclusion of the FAMR is that the underlying reason for the existence of the financial advice gap is that there are not sufficient financial advisers since too many advisers are serving wealthy clients.[70] According to the survey conducted by OpenMoney and YouGov, an increasing number of clients are falling into the financial advice gap.[71] OpenMoney's survey indicates that there are more than 400,000 people who believe they could not afford financial advice and over five million people who are not aware that there is free financial advice that could benefit them.[72] There are six million Britons who would be willing to pay for financial advice if the fee for that advice were lower.[73]

The role of robo-advisers such as Nutmeg and Wealthify is to fill this financial advice gap.[74]Robo-advisers are a type of financial adviser that provides financial advice 'in person' or enables investment management online, with moderate to minimal human intervention. 'Robo-advice' is an umbrella term that refers to a broad spectrum of online automated tools and algorithms to determine financial or investment decisions for an individual's portfolio. This process is based on financial analysis algorithms derived from mathematical rules. Progress through economic modelling and artificial intelligence is the cornerstone of this technology. These algorithms are executed

---

[61] Ji (2017), pp. 1543, 1583.
[62] Study of the Panel of the Future of Science and Technology of European Parliament (2019) on A Governance Framework for Algorithmic Accountability and Transparency.
[63] Kingston (2019).
[64] Kaminski (2019).
[65] Lightbourne (2017) pp 651, 679.
[66] Petrie, http://www.smf.co.uk/wp-content/uploads/2017/06/5599-SMF-Financial-Advice-Gap-Report-WEB.pdf (last accessed on 25 November 2019).
[67] FCA, https://www.fca.org.uk/publication/corporate/famr-final-report.pdf (last accessed on 25 November 2019).
[68] *Ibid.*
[69] *Ibid.*
[70] *Ibid.*
[71] Rach, https://portfolio-adviser.com/robo-advisers-blow-advice-gap-further-apart/ (last accessed on 25 November 2019).
[72] *Ibid.*
[73] See https://www.financialplanningtoday.co.uk/news/item/10261-6m-britons-would-pay-for-cheaper-financial-advice (last accessed on 25 November 2019).
[74] Financial Times, https://www.ft.com/content/1b931788-7be1-11e9-81d2-f785092ab560 (last accessed on 25 November 2019).

by software and thus, taken to extremes, human intervention is not required.[75]

Robo-advisers aim at reducing the cost of financial advisory services, increasing consumer protection by reducing conflicts of interest,[76] providing better rational investment choices,[77] and enabling more access to real-time information.[78] Hence, robo-advisers can enhance the access to finance and reducing the cost of financial access that leads to more affordable financial services.[79] This effect would be highly beneficial for average savers who could access services that were previously inaccessible due to high commission-fees.[80]

2. Risks of conflict of interest, unsuitable products, and design errors

The use of robo-advisers may put an end to two related problems in the financial markets. Financial advisers tend to sell high commission-fee products because the advisers draw their income from their sale.[81] Consequently, there is a conflict of interest between the investor and the adviser, who is also the broker.[82] However, it is possible for the algorithms to be designed to avoid such a conflict.[83] There is also a risk that robo-advisers may promote products that are not suitable for the particular investor. In addition, there is a risk that there may be algorithm design errors that can cause investor losses.[84]

There is clearly potential tension between the broker's interests and the client's interests.[85] Robo-advisers may only be used to provide advice or recommendation, without performing the executions, although the users in these situations are likely to be guided to place orders through a specific product provider. For instance, Scalable Capital- an online robo-advice company, launched over-the-phone and face-to-face consultations for clients to select their investment portfolios based on their level of risk tolerance from a range of suggested advice.[86] Although financial institutions are responsible for damages caused to investors by using or relying on robo-advisers, there are some situations in which financial institutions are not responsible. These are the following: first, when financial institutions become insolvent and there is insufficient money cover to compensate investors; and second, when advice given was regarded merely as 'guidance' and the investor has autonomy to decide whether or not to accept it.[87]

3. Legal framework for protecting investors

Access to finance requires a legal and regulatory framework to protect investors who use robo-advisers for personal or business finance. There are various legal tools that govern the relationship between financial institutions and investors, as well as between developers of AI and investors.

3.1 Contract

---

[75] Ron (2014).
[76] Financial Times, https://www.ft.com/content/f675a6e2-6bf4-11e9-80c7-60ee53e6681d (last accessed on 25 November 2019).
[77] Laboure and Turner (2018).
[78] See http://empirica-software.com/reasons-for-asset-managers-to-implement-robo-adviser-software/ (last accessed on 25 November 2019).
[79] Philippon (2019).
[80] Financial Times, https://www.ft.com/content/1b931788-7be1-11e9-81d2-f785092ab560 (last accessed on 25 November 2019).
[81] HM Treasury (2016); also see Final Report of European Insurance and Occupational Pensions Authority-15/006 of 2015 on Public Consultation on the Draft Technical Advice on Conflict of Interest in Direct and Intermediated Sales of Insurance-based Investment Products.
[82] Edwards (2018), p 97.
[83] Bank of England and FCA (2019).
[84] See https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-risk-algorithmic-machine-learning-risk-management.pdf (last accessed on 25 November 2019).
[85] *Ibid.*
[86] Financial Times, https://www.ft.com/content/f9b8fda4-e1c1-11e7-a8a4-0a1e63a52f9c (last accessed on 25 November 2019).
[87] Stolper and Walter (2017), pp 581, 643; FCA, Understanding 'advice' and 'guidance' on investments https://www.fca.org.uk/consumers/understanding-advice-guidance-investments

In the UK, investors are protected by common law, statutory law, and the regulators' rules. Under common law, investors are protected through contract law, duty of care under tort law, and the fiduciary duty provisions under the law of equity. In contract law, investors are protected by the terms under the contract as well as by the various principles including mistake, misrepresentation, duress, undue influence, and legality.[88] Under the Unfair Contract Terms Act 1977, they are also protected against unfair terms.[89] Therefore, the use of AI devices by advisers should not violate these principles. Furthermore, if the investors are consumers, they will also be protected by consumer protection laws. However, contract law is unlikely to be an effective tool in providing protection to investors who do not have the capacity to appreciate the nature of AI, the performance of it, and whether AI is a suitable device for them to use for making investments.[90] Increasingly, a contract will appear merely as evidence of the existence of an agreement for the conduct between financial advisers and their clients. Prior to an investor's use of AI, the terms of a contract between them and their advisers investors are unlikely to be negotiated between the parties. Investors are unlikely to be sophisticated enough to ask the financial advisers to disclose relevant information before they agree to accept the advice derived from the algorithms. Clients may not even be able to negotiate a specific term that requires their advisers to explain how particular products were selected for them.

3.2 Tort

In tort, the advisers should owe a duty of care to the investors,[91] which entails ensuring that in deploying AI for providing advice or even execution services, the advisers behaviour does not fall short of a standard of care. The difficulty lies in how to identify an appropriate standard of care when using AI. There is currently no such standard set by either the financial services regulators or the industry.[92] Even if the regulators have set out rules to which the investment advisers must comply, these rules do not necessarily form the standard of care that the court will apply in determining whether there is a breach.[93] Relevant questions in setting the standard include: which AI devices are suitable for the client? what kind of data should be fed into an AI device to produce investment advice? what kind of warning should be given to investors? what kind of assistance should be given to investors? what kind of explanation should be given to investors about the outcome of the algorithms?

3.3 Fiduciary duty

The core of fiduciary duty is both duty of loyalty and duty of good faith.[94] Under the duty of loyalty, investor advisers should not place their interests in conflict with those of their clients.[95] This duty should not be removed by contract,[96] as fiduciary duties may generally be altered or restricted by agreement between the parties.[97] In practical terms, advisers need to use their best endeavours to find a suitable investment product for their clients[98] rather than offering products that will reward them with a commission. Compared with duty of care, fiduciary duty applies in more limited circumstances. Fiduciary duty prohibits financial advisers acting in disloyal or improper way, i.e. it is a negative obligation.[99] However, duty of care requires financial advisers to act competently and not recklessly, i.e. it is a positive obligation compared with fiduciary duty.[100] When used in executing the clients' request, AI should be used to fulfil advisers' duty of best execution.[101] While price discrimination is a common practice in market transactions, fiduciary duty is insufficient to remove such a risk.

3.4 Consumer protection is key

Access to finance will require stronger consumer protection to increase consumers' willingness to use robo-advisers. Relying on an ex post regime based on common law is ineffective in providing protection to investors.

---

[88] Cartwright (2006).
[89] Article 2 (Negligence Liability), Unfair Contract Terms Act 1977.
[90] Goodman and Flaxman (2017).
[91] Lipner and Catalano (2009), p 663.
[92] Scherer (2016).
[93] *Ibid.*
[94] See *Bristol & West Building Society v. Mothew* [1998] Ch 1 at 18.
[95] *Ibid.*
[96] Recommendation 7 of "The Kay Review of UK Equity Markets and Long-Term Decision Making" (2012).
[97] FCA DP 18/5 (2018).
[98] Law Commission CP No 350 (2014).
[99] Law Commission CP No 215 (2013).
[100] *Ibid.*
[101] See *infra* n. 65, pp 651, 679.

The FCA stated[102] that if robo-advisers filter products and propose them based upon specific factors relating to a customer's life and/or situation, this amounts to a personal recommendation. Therefore, the entire set of laws related to consumer protection would apply. Consumers are usually deemed to be vulnerable, as they do not understand the mechanisms working in financial markets and also because they cannot fully understand advice provided.[103] As an experimentation space, a 'sandbox' would provide a more suitable environment for the emerging technologies.[104] Firms could then test a new business model built on Fintech without fearing the demanding scrutiny of the FCA.[105] However, it would not be sufficient to use a sandbox to protect consumers. In the US, the SEC charged two robo-advisers with making false disclosures[106].

3.5 Product liability

The institutions, i.e. investment firms, are responsible for damages caused to, or profits gained from investors. As the institutions will be deploying the AI devices, the current law specifies that they are responsible for damages caused to investors,[107] even though the AI devices have been developed by third parties, i.e. a tech company. In line with the approaches taken in the area of algorithmic trading, institutions using algorithmic trading are responsible for the effects caused and are responsible for the initial and continued testing of the algorithms.[108] However, the investor liability that the third parties should assume is not simply a matter for debate. The financial institutions could be insolvent, and there might be inadequate funding to compensate investors, whether provided through insurance or the government's scheme of compensation. There might be an issue of how investors may hold the third-party developers responsible for losses.[109] In the realm of product liability, third parties are strictly liable for consumer losses.[110] However, AI is not a product and may not be used or operated by the consumers themselves. More often than not, AI devices are a set of algorithms (software) used by financial institutions to provide advice or execution for clients. Should the computer scientists and tech developers be responsible for mistakes in the design of the algorithms? The general answer lies in the product liability of the software. The more specific question is whether AI developers should be responsible for any damages caused by the design of AI. The same question also arises in automated vehicles[111] and defence software.[112] The EU Directive 1985[113] imposes strict liability on all parties in the supply chain for defective products, whether or not the defect arose from negligence. The UK law[114] that embodies this directive is not clear on whether software is a product: the application of this law to software might cause a floodgate risk, and due to the widespread use of software, a legal finding that software providers are at fault could lead to unlimited liability.

4. Regulating robo-advisers to achieve access to finance

To enhance financial inclusion through the use of robo-advisers, the AI solutions used must not be inferior to those given and used by wealth management providers to offer services to wealthier clients.[115] The major challenge of retail investors is to make informed decisions based on market information, such as fundamental aspects of companies, the industry specificities, market competition, and macro-economic conditions. Average investors are not normally equipped with professional expertise or the time to collect and analyse these data. By contrast, the wealthier investors with the help of professional financial advisers could make better data-driven investment decisions. In the UK, after a free introductory session, typical independent financial advisers' fees are £450 for advice in a £11,000 investment asset scale; and £1,500 for investment strategy advice for a £50,000

[102] Baker and Dellaert (2018), p 1740.
[103] Edwards (2018), p 97.
[104] FCA (2017).
[105] Ringe and Ruof (2018).
[106] See https://www.sec.gov/news/press-release/2018-300 (last accessed on 25 November 2019).
[107] Cerka et al. (2015), pp 376, 389.
[108] FCA, https://www.fca.org.uk/mifid-ii/8-algorithmic-and-high-frequency-trading-hft-requirements (last accessed on 25 November 2019).
[109] See *infra* n. 63.
[110] Section 2(1), the Consumer Protection Act 1987.
[111] Kim (2018), pp 300, 317.
[112] Vihul, https://ccdcoe.org/uploads/2018/10/TP_02.pdf (last accessed on 25 November 2019).
[113] EU Directive 85/374/EEC on liability for defective products (Product Liability Directive).
[114] Part 1, the Consumer Protection Act 1987 (Consumer Protection Act).
[115] Langridge, https://www.morganmckinley.com.au/article/how-ai-levels-playing-field-smes (last accessed on 25 November 2019).

inheritance.[116] AI should be used to level the playing field.[117] The World Bank's research indicates that the asset amount under the management of robo-advisers will be tripled in the US from 426 billion in 2018 to 1,486 billion US Dollars in 2023.[118] For retail investors, robo-advisers are in place to reduce minimum investment requirements, even to no minimum investment criteria at all, as in the case of Betterment, and to charge lower fees, normally 0.25 per cent of managed assets for robo-advisers and 0.75 to 1.5 per cent of managed assets for human advisers. This is because robo-advisers save on fixed costs, such as the salaries of financial advisers, and reduce behavioural biases, such as limited capacity to manage and invest in various categories of assets.[119] The Bank of America requires $25,000 US to create an account with private financial advisers, compared with $ 5,000 US to create an account with robo-advisers.[120] In addition, robo-advisers can easily be accessed at any time and from anywhere.[121]

In terms of redress, consumers are less likely to bargain for their terms and are less likely to bring law suits to recover compensation, due to the excessive costs of bringing lawsuits.[122] Therefore, there must be more ex ante control in the design, development, and deployment of the robo-advisers used, and a more robust complaint or compensation scheme for consumers should be implemented.[123]

Part III AI as RegTech

1. RegTech and SupTech in financial markets

Since AI can streamline KYC/CDD processes to reduce the compliance costs of financial intermediaries[124], more investment firms could be set up to provide services to investors. This would increase market competition and allow more financial innovation and thereby provide better access to finance for consumers and investors.

AI devices can be used to detect conduct that violates market integrity, such as market manipulation including price fixing, disinformation, insider dealing, and money laundering. AI devices can be used by financial institutions, regulators, policy-makers, or even private market watchdogs to detect and prevent such misconduct. When devices are used for this purpose, they are dubbed 'regulatory technology' (RegTech[125]). RegTech will also include SupTech that is mainly used for the purpose of market supervision.[126] When RegTech is used to detect market misconduct, it involves elements of market surveillance that include the collection of individual data.[127] In this situation, the value of protecting individual rights and dignity may conflict with market integrity and public interest. For instance, an anti-money laundering regime requires financial intermediaries to screen personal data. However, this may be in contravention with the spirit of the General Data Protection Regulation (GDPR).

The main objective of RegTech is to protect market integrity. AI has been used as a SupTech service by exchanges,[128] in providing supervision and as a RegTech service by financial institutions,[129] for compliance

[116] *Ibid.*
[117] *Ibid.*
[118] The World Bank (2019), http://documents.worldbank.org/curated/en/275041551196836758/pdf/Robo-Advisers-Investing-through-Machines.pdf (last accessed on 25 November 2019).
[119] *Ibid.*
[120] *Ibid.*
[121] *Ibid.*
[122] Polinsky and Shavell (2010), https://pdfs.semanticscholar.org/bc7a/62029d2eb48719140b1e32f2b7141473a88e.pdf?_ga=2.52763693.481831465.1565280574-211989861.1563719626 (last accessed on 25 November 2019).
[123] Scherer (2016), pp 353, 400; also see https://theconversation.com/whos-to-blame-when-artificial-intelligence-systems-go-wrong-45771 (last accessed on 25 November 2019).
[124] Kingston (2017).
[125] According to the definition given by FCA, "RegTech applies to new technologies developed to help overcome regulatory challenges in financial services", https://www.fca.org.uk/firms/regtech (last accessed on 25 November 2019).
[126] Armstrong, https://www.esma.europa.eu/sites/default/files/library/esma71-99-1070_speech_on_regtech.pdf (last accessed on 25 November 2019).
[127] Broeders and Prenio (2018).
[128] See *infra* n. 126.
[129] See https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (last accessed on 25 November 2019).

purposes. In addition to ensuring the previously mentioned appropriate design modes in investor protection, another emerging concern is the need for data governance that ensures privacy protection and data protection.[130] In this case, to ensure market integrity, data on individuals can be collected that relates to law enforcement-related activities, such as insider dealing, market manipulation, and money laundering.[131] Personal data, transaction/order book data, communications and suspicious transaction and order reports (STORs) are collected for market oversight.[132]

The collection of personal data for RegTech may violate data protection rules and privacy rights.[133] While consent is required for controlling and processing data, data collected for market integrity can be processed and transferred without the consent of the individual.[134] That is to say, individuals may not have the right to prevent the unauthorized sharing of their personal information in accordance with the GDPR and Data Protection Act 2018.[135] The right of privacy can be violated when personal data are collected for the development and deployment of RegTech.

2. AI and Anti-Money Laundering (AML)

Some regulators are using AI for fraud and AML/CFT detection.[136] It is possible, for example, that Machine Learning (ML) algorithms could detect suspicious transactions and provide a risk score for such transactions through supervised learning.[137] In addition, ML could be applied to screen known criminals, individuals and institutions who are on the global "black-list" and forecast the likelihood of money laundering.[138] Furthermore, unsupervised machine learning allows it to summarise the characteristics of variables and to tag them based on certain criteria established by unsupervised learning.[139] That is to say, through unsupervised machine learning, financial institutions and regulatory authorities could identify the behavioural characteristics of financial crimes, including money laundering. The Australian Securities and Investments Commission (ASIC) has been exploring the quality of results and the potential use of Natural Language Process (NLP) technology to identify and extract entities of interest from evidentiary documents.[140] ASIC is using NLP and other technology to visualise and explore the extracted entities and their relationships. To fight criminal activities carried out through the banking system (such as money laundering), detailed information on bank transfers are collected and this information correlated with information from newspaper articles.[141] Similarly, the Monetary Authority of Singapore (MAS) is exploring the use of AI and machine learning in the analysis of suspicious transactions to identify those transactions that warrant further attention,[142] allowing supervisors to focus their resources on higher risk transactions. Investigating suspicious transactions is time consuming. Regulated entities use defensive filings to protect themselves, [143] and this leads to a high rate of false positives.[144] Machine learning is being used to identify complex patterns and highlight suspicious transactions that are potentially more serious and warrant closer investigation.[145] Coupled with machine learning methods to analyse the granular data from transactions, client

[130] See https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence (last accessed on 25 November 2019).
[131] FCA, https://www.fca.org.uk/privacy/personal-data-and-market-oversight (last accessed on 25 November 2019).
[132] *Ibid.*
[133] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/(last accessed on 25 November 2019).
[134] Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last accessed on 25 November 2019).
[135] FCA, https://www.fca.org.uk/privacy/personal-data-and-market-oversight (last accessed on 25 November 2019).
[136] FSB, https://www.fsb.org/wp-content/uploads/P011117.pdf (last accessed on 25 November 2019).
[137] Deloitte, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance/sea-fas-deloitte-uob-whitepaper-digital.pdf (last accessed on 25 November 2019).
[138] *Ibid.*
[139] *Ibid.*
[140] FSB, https://www.fsb.org/wp-content/uploads/P011117.pdf (last accessed on 25 November 2019).
[141] See https://gomedici.com/risk-management-most-important-application-of-ai-in-financial-sector (last accessed on 25 November 2019).
[142] *Ibid.*
[143] See *infra* n. 8.
[144] See https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Singapore-2016.pdf.
[145] *Ibid.*

profiles, and a variety of unstructured data, machine learning is being explored to uncover non-linear relationships among different attributes and entities and to detect potentially complicated behaviour patterns of money laundering and terrorism financing that are not directly observable through suspicious transaction filings from individual entities.[146]

3. KYC of Fund and asset management

Funds and other methods of investment, such as AIFs (alternative investment funds), attract a large number of organisations and individuals to invest. When individual investors or corporations make investments, they may also be requested to provide their personal information—including their names, address, date of birth, contact information, related anti-money laundering information, documents of income certification, payment details for dividend and redemption proceeds, and tax residence information. They are collected for different purposes, such as identification or to guarantee an obligation. [147] Thus, personal information is being controlled, processed and stored not only by investment fund companies, management companies or transfer agencies but also by the directors of these companies or other third-party agencies working for them.

To guarantee the security of fund transactions, MiFID II requires fund companies to reinforce six aspects of data collection.[148] For example, to prevent money laundering, customers may be asked to provide a certification of income. Furthermore, the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 requires firms to maintain the safe custody of assets belonging to their clients.[149] Under these regulations, firms should establish and keep at least five years' records with as much detail as possible.[150] This includes personal information regarding relationships, order handlings, reports, assets and so forth.[151] However, GDPR authorizes the right of data subjects to have their personal data erased without delay.[152] The data subject has the right to demand the information controller to erase personal data concerning him or her without undue delay and the information controller has an obligation to do so.[153] This principle conflicts with the MiFID II principle that requires a firm to retain all records kept by it in relation to its MiFID business for a period of at least five years".[154] The purpose of the information collected is paramount. Are it being collected for law enforcement purposes, for guarantee obligation, for developing new products, or for research purposes such as developing RegTech?

4. Streamlining compliance processes

The KYC process is often costly, laborious, and highly duplicative, covering many services and institutions.[155] According to Thomson Reuters, some major financial institutions spend 500 million US dollars on KYC and CDD annually; the annual spending of 10 per cent of world's top financial institutions are at least 100 million dollars and the average is 48 million dollars globally.[156] Machine learning is increasingly used in the remote KYC processes of financial services firms to perform identity and background pre-checks. For example, applying AI in the process of KYC could detect any attempt to use fake documents to perform KYC in real-time. AI could complete the facial, documental and any other verifications in real-time in a single cycle. Hence, AI helps financial institutions to perform AML background checking in real-time to avoid unwanted regulatory scrutiny and

---

[146] See *infra* n. 8.
[147] Deloitte, https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/GDPR%20for%20Funds%20FINAL.pdf (last accessed on 25 November 2019).
[148] "ESMA (2014).
[149] FCA, https://www.fca.org.uk/firms/money-laundering/safe-custody-services (last accessed on 25 November 2019).
[150] *Ibid.*
[151] Varney and Malna, https://www.burges-salmon.com/news-and-insight/legal-updates/how-to-align-mifid-ii-and-gdpr-when-processing-client-data/ (last accessed on 25 November 2019).
[152] Article 17, GDPR.
[153] Art. 17 (1), GDPR
[154] SYSC 9.1.2
[155] John Callahan, https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/#1f3fe9a98dbb (last accessed on 25 November 2019).
[156] *Ibid.*

monetary fines.[157] Machine learning is predominantly used in two ways: (1) evaluating whether images in identifying documents match one another, and (2) calculating the risk scores on which firms determine which individuals or applications need to receive additional scrutiny. Machine learning-based risk scores are also used in ongoing periodic checks based on public and other data sources, such as police registers of offenders and social media services.[158]

Use of these sources may enable risk and trust to be assessed quickly and cheaply.[159] Firms can use risk scores on the probability of customers raising "red flags" on KYC checks to help make decisions on whether to proceed with the time and expense of a full background check. Nonetheless, concerns about the tools' accuracy have kept some financial services from incorporating them. Research is needed to discover how regulators accept this kind of approach and what their worries are.

5. Public interest and individual right

For public enforcement agencies, such as the National Crime Agency, the Serious Fraud Office, FCA, and policing agencies, current data protection law aimed at protecting individual sensitive data does not prevent them from collecting that information for the purpose of law enforcement.[160] Furthermore, the current law does not prevent public agencies or financial institutions from collecting individual data in the public domain, and that can help them construct an individual profile for the purpose of KYC, as well as for the detection of suspicious transactions.[161] However, the ethical foundations of individual profiling for market surveillance have not yet been robustly established.[162] The identification of the parameters for agencies—either public or private—to carry out individual profiling will need to be built on human rights and human dignity principles[163] to ensure not only individual safety but also societal safety.[164] Such profiling information could fall into the wrong hands and be used maliciously.[165]

Individual consent is inadequate in protecting the individual for the following reasons: first, a person, as a general principle, cannot consent to be harmed;[166] second, the individual may not appreciate the risk, [167]; and third, the individual may not know to what he or she is consenting[168]. Hence, there is also a need to redefine individual consent: the method of consent, the purpose of consent, and the possible revision and withdrawal of consent.[169]

Even for KYC processes conducted for the purpose of protecting the individual, such as assessing the clients' risk appetite in accordance with the clients' suitability rules[170], the consent to individual profiling is also problematic. The problem can arise in data quality and accuracy that can affect the quality and accuracy of profiling.[171] The

[157] Imran, https://dzone.com/articles/how-artificial-intelligence-can-revolutionise-kyc (last accessed on 25 November 2019).
[158] See *infra* n. 6.
[159] *Ibid.*
[160] Article 6.1 (c and f), GDPR; also see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/ (last accessed on 25 November 2019).
[161] Article 6.1 (e), GDPR; also see PWC, https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-anti-money-laundering-know-your-customer-quick-reference-guide.pdf (last accessed on 25 November 2019).
[162] Information Commissioner's Office, https://ico.org.uk/media/about-the-ico/documents/1042386/surveillance-report-for-home-select-committee.pdf (last accessed on 25 November 2019).
[163] Bernal (2016), pp 243, 264.
[164] van den Hoven (2010), pp 60, 76; *also see* EU Ethics guidelines for Trustworthy AI. See Respect for democracy, justice and the rule of law; and The Principle of Prevention of Harm.
[165] Ahmed (2014), pp 986, 988.
[166] Tadros (2011), pp 23, 49. The Principle of Prevention of Harm under EU Ethics Guidelines for Trustworthy AI. The validity of consent to harm depends on the content of what is consented to and it is valid in some circumstances; also see Boddington (2017), pp 90, 92.
[167] Humerick (2018), p 405.
[168] *Ibid*, pp 405, 406.
[169] *Ibid*, p 407.
[170] Tadros (2011), pp 23, 49. The Principle of Prevention of Harm under EU Ethics Guidelines for Trustworthy AI. The validity of consent to harm depends on the content of what is consented to and it is valid in some circumstances; also see Sarangi and Sharma (2018).
[171] Sherman (2015).

data could be collected via social media and other smart devices. These integrated datasets containing information about an individual, possibly with extended information, can easily be seized by third parties through a legal request, e.g. a request from a foreign government. Since clients did not consent to the sharing of their datasets with third party government agencies, transferring these data or providing government agencies access to those datasets may have prejudicial effects on the individuals' rights in the legal process.[172] For instance, the original data collector, even if fully complying with statutory obligations initially, will still breach its legal obligations if they share data with next public authority to process these data further, unless the first collector provided a detailed explanation of further sharing of the data and obtained consent at the time of collection.[173]

6. Policy recommendation

In this article, the author has looked at the regulatory objectives and regulatory methods associated with management systems and processes where AI has been deployed in securities trading and investment services. The author uses HFT as an example to examine how AI is regulated on a trading platform that is not consumer facing. The primary regulatory objective is to deal with systemic risk—flash crashes, liquidity risks, and procyclical behaviour. The secondary objective is investor protection (fairness) against market manipulation. The main regulatory approach is the requirement that operators—HFT specialist firms, securities firms, proprietary traders, and trading venues—have internal risk management systems and processes. In this way, these operators are also required to consider market safety and market integrity. Whether HFTs should disclose algorithms to the regulators remains a contentious issue, and the UK regulators do not require such disclosure. The regulatory objective of market safety is appropriate as the basis for continuing the regulation of AI for trading platforms. However, HFT firms, securities firms, and trading venues are all being subjected to a higher degree of control by regulators. These methods of regulation may not be appropriate for newcomers in the development of AI Fintech services provided on p2p trading platforms. The new p2p trading platforms, either on a DLT network or on Amazon-like ones, will need more consumer protection including price discrimination and privacy rights' protection.

In a p2p trading platform where consumers trade securities, the same regulatory objectives of market safety and market integrity should apply. The platform providers who use algorithms to execute client transactions, such as distributing their portfolios, need to ensure the protection of clients. To ensure there is no market manipulation behaviour, including price manipulation and price discrimination, the platform providers will also need to bear the burden of identifying those who use algorithms to trade or allocate securities. Unlike regulated trading platforms, the users of p2p platforms are likely to be individuals who rely on algorithms developed for interactions on the platforms. It is unlikely that individuals will have the capacity to implement risk management systems and controls. Therefore, to increase financial inclusion, the onus will be on the trading platform to monitor operations and to set the parameters of where these algorithms will operate. There should be an effective mechanism to exclude anybody from participating in the platforms who is found to be using algorithms to cause systemic problems or to manipulate the market.

Part II discussed protection to investors from asset managers and investment advisers who are using AI. Since asset managers and investor advisers (even online ones) are more consumer facing, more protection should be given to investors, particularly retail and consumer investors, to increase their willingness to use robo-advisers to manage their assets. It is unlikely that investors will be able to negotiate contractual terms that serve to protect them against potential harm such as misleading information and price discrimination. The standard of care under tort law in financial services is an unstable concept for investors to use to claim redress. Furthermore, it is not clear whether fiduciary duty can be assumed by robo-advisers or by advisers using algorithms.[174] Fiduciary duties can also be altered and restricted by parties. A fiduciary duty concerns what a fiduciary (investment adviser) cannot do (conflict of interest) rather than should do (act in the best interest of the client).

Therefore, using common law principles to provide protection to consumer investors would be inadequate, particularly if AI aims to provide access to finance and to close the advice gap where less wealthy investors do not have access to the same advice services as the wealthier. Wealthier investors are not only able to rely on common law principles to control the level of their protection but are also more likely to make complaints and bring lawsuits. It is more likely that statutory protection based on policy will provide consumers with protection

[172] Law Commission Consultation Paper No 214 (2013).
[173] O'Shea, https://byrnewallace.com/assets/components/uploads/Data%20Sharing%20in%20the%20Public%20Sector.pdf (last accessed on 25 November 2019); also see Johnny (2018).
[174] See http://classic.austlii.edu.au/au/journals/SydLawRw/2018/3.html (last accessed on 25 November 2019).

that can balance the need of closing the advice gap with that of financial innovation. For instance, the 'best interest' principle and the suitability principle should continue to apply to the use of AI for providing advice on execution and investment. Detriments to consumers' welfare such as price discrimination—wealthier clients' investments are sold at a higher price—should also be factored in.

In terms of user protection, the more problematic situation is the one in which an AI investment advice tool is provided online—freely downloadable—and can be used on the providers' platform or other platforms. These tools may not have been developed in-house by the investment firms. The advice may simply provide free guidance. In this situation, it is difficult to argue that there is a fiduciary relationship between a firm using robo-advisers and consumers/investors. There can also be a question about whether a contract is formed if the robo-advisers provide free investment guidance. Furthermore, it is likely that the software will continue to be treated as 'non-product', hence product liability rules do not apply. These factors could leave investors relying on robo-advisers without adequate protection.

Rather than traditional investment services, consumers may use online robo-advisers to purchase financial products that might otherwise be unavailable to them, because they do not have access to the information that wealth management advisers provide. With open data and the development of more sophisticated algorithms, users may select online advisers that provide more economic services for advice and investment portfolio management. Consumers should be protected against poorly developed algorithms that do not act in their best interest, that are prejudiced against them, or that cause damage through errors.

In Part III, the focus is on using AI in RegTech or SupTech solutions for preventing, detecting, and controlling financial crime, such as money laundering. Due to the cost of compliance, many online financial firms are prohibited from giving financial advice, especially if they process transactions on behalf of clients or if they provide p2p investment platforms. RegTech will streamline the KYC/CDD processes and hence reduce their compliance costs. This, in turn, will allow more firms to come to the market to offer services. The regulatory objective of market integrity directly conflicts with the privacy rights of individuals and data protection laws. It is submitted that data governance will need to be established to protect individual rights but also societal safety.

Conclusion

AI will bring benefits and risks to the financial services sector. To ensure continuity, market safety, investor protection, and market integrity should continue to guide the regulation of AI. In addition to these, access to finance should be a regulatory objective so that AI can be used to not only benefit financial intermediaries but also to provide a larger social benefit to those previously excluded from financial opportunities. Access to finance will help the use and regulation of AI to gain wider public acceptance. For this objective, AI can be used to help the optimisation of capital on p2p platforms, help consumers to have cheaper access to more information through robo-advisers, and through the use of RegTech services to streamline KYC/CDD processes, hence reducing compliance costs. More detailed rules need to be developed to certify good algorithms and good platforms, to strengthen ex ante and increase ex post the protection to individuals who use robo-advisers, and to address how individual rights, such as privacy rights and data rights, can be protected to allow the conducting of more efficient KYC processes.

GET IN TOUCH

Contact us to arrange a personal consultation

Email: studyonline@manchester.ac.uk

www.manchester.ac.uk/techlaw