Legal risks of using regulatory technologies in business and professional activities

Olga Sushkova*

Kutafin Moscow State Law University (MSAL), Moscow, Russia

Abstract. When using artificial intelligence technology in RegTech or SupTech solutions to prevent, detect and control financial crimes such as money laundering, it is necessary to be aware that due to compliance costs, many online financial firms are prohibited from providing financial advice, especially if they process transactions on behalf of clients or provide p2p investment platforms. RegTech streamlines KYC/CDD processes and therefore has the ability to reduce compliance costs. This, in turn, will allow more firms to enter the market to offer services. The regulatory goal of ensuring market integrity directly conflicts with the rights of individuals and the Data Protection Acts. It is argued that data governance will need to be established to protect individual rights and public safety. Furthermore, the question remains unresolved as to whether fiduciary duties can be assumed by robo-advisors or consultants using algorithms. Fiduciary duties may also be modified and limited by the parties. The fiduciary duty concerns what the fiduciary (investment adviser) cannot do (conflict of interest) but should not do (act in the best interest of the client). Consequently, the use of common law principles to protect consumer investors is currently underdeveloped, particularly if the AI seeks to provide access to finance and fill gaps in guidance.

1 Introduction

As Artificial Intelligence (hereinafter referred to as AI) can optimize KYC (Know Your Customer)/CDD processes to reduce the compliance costs of financial intermediaries, it can also create more investment firms to provide services to investors [1]. This will increase competition in the market, allow for more financial innovation, and improve access to finance for consumers and investors [2]. The development of financial innovation will increase the growth rate of the country's economy; increase the availability of capital; strengthen the national position in the global economy [3].

AI technologies can be used to identify activities that compromise market integrity, such as market manipulation, including price-fixing, misinformation, insider trading, and money laundering. In addition, such AI technologies can be used by financial institutions, regulators, and private market observers to detect and prevent misconduct. When such AI technologies are used for this purpose, they are called Regulating Technologies (RegTech) [4]. RegTech will also include SupTech, which is mainly used for market surveillance purposes [5]. When

* Corresponding author: ovsushkova@msal.ru

RegTech is used to detect market misconduct, it includes elements of market surveillance that includes the collection of individual data.

Shevchenko O.M. distinguishes two types of market manipulation of financial services, using the actions that are subject to administrative or criminal liability [6].

The first type - information manipulation - in Russia, this is market manipulation through the dissemination of deliberately false information - deliberate dissemination through mass media with unrestricted access (including the Internet) or through any other means of deliberately false information that caused price, demand, supply or trade volume of financial instruments, foreign currency, and/or goods to deviate from the level or support significantly different from from the level that would have developed without the dissemination of such information.

The second type is market manipulation through transactions in organized trading (trade manipulation). The Law 224-FZ [7] provides for 6 types of such manipulations, which differ not only in the ways they are committed but also in the consequences and types of organized trading where they are committed.

2 Methodological basis of the study

This paper has applied the following regulatory methods related to the management systems and processes in which AI is applied in securities trading and investment services through general scientific principles and approaches. HFT is used as an example, to explore how AI is regulated on a non-consumer-oriented trading platform. The main purpose of regulation is to deal with systemic risks - sudden failures, liquidity risks, and pro-cyclical behavior. A secondary goal is to protect investors from market manipulation. The main regulatory approach requires operators - specialist HFT firms, securities firms, private traders, and trading venues - to have internal risk management systems and processes in place. Thus, these operators are also required to consider the security and integrity of the market.

A comprehensive approach and comparative research method identified the regulatory objective of market security, which is the basis for the continued regulation of AI for trading platforms. However, HFT firms, securities firms, and trading venues are subject to higher regulatory scrutiny. These regulatory methods may not be appropriate for those developers who provide AI FinTech services operating on p2p trading platforms. New p2p trading platforms, whether on a distributed ledger technology (DLT) network or networks like Amazon, will require greater consumer protections, including price discrimination and privacy rights protections. In a p2p trading platform where consumers trade securities, security and market integrity should apply the same regulatory goals. Platform providers that use algorithms to perform client transactions, such as allocating their portfolios, must ensure that clients are protected. To ensure there is no manipulation of the market, including price manipulation and price discrimination, platform providers will also need to bear the burden of identifying those who use algorithms to trade or distribute securities. Unlike regulated trading platforms, users of p2p platforms are likely to rely on algorithms designed to interact on the platforms. Individuals are unlikely to be able to implement risk management systems and controls. Consequently, to increase financial inclusion, the trading platform will monitor transactions and set parameters for where these algorithms will operate. There must be an effective mechanism in place to exclude participation in the platforms by anyone found to be using algorithms to create systemic problems or to manipulate the market.

3 Main part

In this situation, the value of protecting individual rights and dignity may conflict with market integrity and the public interest [8]. However, this may be contrary to the spirit of the General Data Protection Regulation (GDPR) [9]. RegTech's primary goal is to protect the integrity of the marketplace. Exchanges use AI as a SupTech service [10], and as a RegTech service by financial institutions [11]. In addition to providing the previously mentioned suitable development regimes to protect investors' rights, another emerging challenge is the need for data governance that protects privacy and data protection [12].

Collecting personal data for RegTech may violate data protection rules and privacy rights [13]. While consent is required for data control and processing, data collected for market integrity may be processed and transmitted without the individual's consent. Individuals may not have the right to prevent unauthorized sharing of their personal information under the GDPR and the Data Protection Act 2018. [14] The right to privacy may be violated when personal data is collected for RegTech development and deployment.

4 Artificial intelligence and the fight against money laundering

Some regulators use AI for fraud detection and anti-money laundering, and counter-terrorist financing (AML/CTF) [15].

It appears that self-learning software and digital analytics as a mandatory regulatory requirement for systems aimed at combating money laundering, terrorist financing in the next 5-10 years. Here it should noted that money launderers will also use software to build the logistics of money laundering and terrorist financing transactions [16].

Using AI and self-learning software concerning AML/CFT state financial control for business and professional entities [17] raises several questions, which are not yet answered by the international community either.

First, how much confidence can be placed in the conclusions and recommendations that the AI will convey?

Second, how can the effectiveness of AI performance be verified, and what legal criteria should be used for such evaluation?

Third, to what extent should AI be integrated into the financial monitoring agent's procedures? Should the AI replace it completely or partially? What requirements should the state financial supervisory authority have for AI systems? Similar questions are asked by foreign financial control authorities [18].

Finally, it is imperative to define the distinction between the areas of responsibility of an AI and a financial monitoring officer, body, or agent [19].

The Australian Securities and Investments Commission (ASIC) is investigating the quality of results and the potential use of natural language processing (NLP) technology to identify and extract items of interest from evidentiary documents [20]. ASIC uses NLP and other technologies to visualize and explore their essence and emerging relationships. To combat criminal activities conducted through the banking system (e.g., money laundering), detailed information on bank transfers is collected, and this information is correlated with information from newspaper articles. Similarly, the Monetary Authority of Singapore (MAS) explores the use of AI and machine learning in analyzing suspicious transactions to identify those transactions that require further attention [21], allowing supervisors to focus their resources on higher-risk transactions. It takes a long time to investigate suspicious transactions.

5 Optimization of compliance processes

The KYC process is often costly, time-consuming, and duplicative, involving many services and agencies [22]. According to Thomson Reuters, some major financial institutions spend $500 million annually on KYC and CDD; the top 10% of financial institutions worldwide spend at least $100 million annually, with an average of $48 million globally. For example, the application of AI in the KYC process can detect any attempt to use forged documents to perform KYC in real time. The AI could perform facial, documentary and any other checks in real time in a single cycle. Thus, AI helps financial institutions perform background checks, and machine learning is used to ensure that in real-time to avoid unwanted inspections by regulators and monetary penalties.

Machine learning is used in two instances: (1) when assessing whether images in identifying documents match each other, and (2) when calculating risk assessments by which firms determine which individuals or applications need additional verification.

Money-laundering-based risk assessments are also used in ongoing periodic checks based on publicly available and other data sources, such as police offender registries and social media services [23]. Using these sources can allow for a quick and cheap assessment of risk and confidence. Thus, research is now needed to determine how regulators are adopting this approach and their concerns.

6 Study results

Current legislation does not prohibit government agencies or financial institutions from collecting individual data in the public domain, which can help them build a customized profile for KYC purposes and detect suspicious transactions. However, the ethical basis for individual profiling for financial market supervision, to date, is not only firmly established but also spot regulated. The setting of parameters for agencies should be based on human rights and principles of human dignity to ensure individual and community safety [24]. Such profile information could fall into the wrong hands and be used maliciously.

Individual consent is insufficient to protect an individual for the following reasons: firstly, an individual cannot, on general constitutional principles, consent to harm; secondly, an individual may not be aware of the risk; and thirdly, an individual may not know what and, what he or she is consenting to. Consequently, [25] there is also a need to revise the definition of 'individual consent' and develop clear criteria for determining the consent method, the purpose of consent, and the possible review and withdrawal of consent.

Even for KYC processes conducted to protect the individual, such as assessing clients' risk appetite under client eligibility rules, consent to individual profiling is also problematic. Problems can arise with the quality and accuracy of the data, affecting the quality and accuracy of the profiling. Data can be collected through social media and other smart devices. These integrated datasets containing information about an individual, possibly with enhanced information, can be easily seized by third parties upon legal requests, such as a request from a foreign government.

As clients have not consented to share their datasets with third-party government agencies, transferring these data or making them available to government agencies and gaining access to these datasets could have detrimental consequences for citizens' rights in litigation (or in bankruptcy) [26]. For example, the initial data collector, even with full compliance with statutory obligations at the outset, would still breach its legal obligations if it shared data with the next government agency for further processing of that data if the first collector did not provide a detailed explanation of further data sharing and did not obtain consent at the time of collection [27].

7 Discussion of the results of the study

Analyzing the situation with digital banking in Russia, O.A. Tarasenko rightly notes that "the availability of remote customer identification affects the growth of digital banking, so banks in all countries are looking for ways to implement such tools. Two key areas of technology development in this area should be noted. The first direction is the proliferation of "single identification" systems, whereby a person once identified by a bank is considered to be identified to others. The second direction is the development of biometrics" [28].

Russia has had a Unified Biometric System (UBS) in place since 2018, with Rostelecom as the operator and the Russian Ministry of Digital Development, Communications, and Mass Media as the regulatory body. According to the Central Bank's Financial Inclusion Strategy, Tarasenko O.A., the purpose of the UBS is to digitalize financial services, make financial services more accessible to consumers, and increase competition in the financial market.

In foreign jurisdictions, funds using specific investment techniques, such as AIFs (alternative investment funds), attract many organizations and individuals to invest. When individual investors or corporations make investments, they may also be asked for their personal information, including personal details, proof of income, details of dividend payments, and repayment details. proceeds and tax residency information. They are collected for various purposes, such as identification or assurance of commitment [29]. Thus, personal information is controlled, processed and stored not only by the investment fund companies, management companies or transfer agencies, but also by the directors of these companies or other persons.

To guarantee the security of fund transactions, MiFID II requires fund companies to use six data collection criteria [30]. For example, to prevent money laundering, clients may be asked to provide a certificate of income. In addition, the Anti-Money Laundering, Counter-Terrorist Financing, and Transfer of Funds Regulations 2017 require companies to ensure that assets belonging to their customers are held securely. According to these provisions, companies must keep records for at least 5 years with as much detail as possible [31]. This includes personal information regarding relationships, order processing, reports, assets, etc. To delete personal data without undue delay is the duty of the information controller (Art. 17(1), GDPR). This principle conflicts with MiFID II, which requires a company to retain all records held by it concerning its MiFID business for a period of at least 5 years. (FCA's Systems and Control Sourcebook). The purpose of the information collected is paramount.

8 Conclusion

AI will bring benefits and risks to the financial services sector. AI should continue to be regulated to ensure continuity, market safety, investor protection, and market integrity. In addition to this, access to finance should be a regulatory goal so that AI can be used to benefit financial intermediaries and provide greater social benefit to those who were previously financially disenfranchised. Access to finance will help the use and regulation of AI gain wider public acceptance. For this purpose, AI can optimize capital on p2p platforms to help consumers have cheaper access to additional information through robo-advisors and by using RegTech services to streamline KYC/CDD processes, which reduces compliance costs. More detailed rules are needed to certify good algorithms and good platforms, strengthen ex-ante and ex-post protections for individuals using robo-advisors, and address how individual rights, such as privacy rights and data rights, can be enforced, protected to conduct more effective KYC processes.

References

1. J. Kingston, Artif Intell Law **25**, 429 (2017)
2. I.V. Ershova, General provisions on self-regulation of business and professional activities. Chapter 2. Self-regulation of entrepreneurial and professional activity: textbook. M.: Prospect, 35 (2020)
3. R.O. Voskanyan, T.V. Vaschenko, Azimuth of Scientific Research: Economics and Management **4(21)**, 75 (2017)
4. According to the definition given by FCA, 'RegTech applies to new technologies developed to help overcome regulatory challenges in financial services'. FCA (2017a) RegTech. https://www.fca.org.uk/firms/innovation/regtech.
5. P. Armstrong, Developments in RegTech and SubTech. https://www.esma.europa.eu/sites/default/files/library/esma71-99-1070_speech_on_regtech.pdf (2018)
6. O.M. Shevchenko, *Legal regulation of the securities market and collective investments*: textbook, 372 (2021)
7. Federal Law of 27.07.2010 No. 224-FZ (as amended on 01.04.2020) "On Counteracting the Unlawful Use of Insider Information and Market Manipulation and on Amending Certain Legislative Acts of the Russian Federation" // Collected Legislation of the Russian Federation. 2010. No. 31. Art. 4193.
8. Yu. G. Leskova, Jurist **11**, 13 (2013)
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation) OJ L 119/1 (2016)
10. M. Polinsky, S. Shavell, Harvard Law Rev. **123**, 1437 (2010)
11. Information Commissioners Office (2017) Big data, artificial intelligence, machine learning and data protection. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.
12. O.V. Sushkova, *Features of the influence of the institution of protection of commercial information and personal data on innovations developed by startups*. In the book: Digital transformation: challenges to law and vectors of scientific research: monograph, under total. ed. A.N. Savenkov; otv. ed. T.A. Polyakova, A.V. Minbaleev. M .: Prospect, 159 (2021)
13. Information Commissioners Office (2019b) Data protection by design and default. 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 /
14. FCA, Personal data and market oversight. Last updated 15 May 2020. https://www.fca.org.uk/privacy/personal-data-and-market-oversight. Accessed 5 Oct 2020 (2018a)
15. Deloitte, The case for artificial intelligence in combating money laundering and terrorist financing: a deep drive into the application of machine learning technology. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance/sea-fas-deloitte-uob-whitepaper-digital.pdf (2018)
16. Federal Law of 07.08.2001 No. 115-FZ (as amended on 30.12.2020) "On Counteraction to Legalization (Laundering) of Criminally Obtained Incomes and Financing of Terrorism" // Collected Legislation of the Russian Federation. 2001. No. 33 (part I). Art. 3418
17. M.Yu. Chelyshev, A.V. Mikhaylov, The Rule of Law **1(13)**, 54 (2013)

18. Speech by Rob Gruppetta, Head of the Financial Crime Department at the FCA, delivered to the FinTech Innovation in AML and Digital ID regional event, London // https://www.fca.org.uk/news/speeches/using -artificial-intelligence-keep-criminal-funds-out-financial-system
19. K.T. Anisina, B.G. Badmaev, I.V. Bit-Shabo and others, *Financial law in the context of the development of the digital economy*: monograph; ed. I.A. Tsindeliani. M .: Prospect, 36 (2019)
20. FSB, Artificial intelligence and machine learning in financial services: market developments and financial stability implications. https://www.fsb.org/wp-content/uploads/P011117.pdf (2017)
21. Medici, Risk management: the most important application of AI in the financial sector. https://gomedici.com/risk-management-most-important-application-of-ai-in-financial-sector (2018)
22. J. Callahan, Know your customer (KYC) will be a great thing when it works. https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/#1f3fe9a98dbb (2018)
23. FSB, Artificial intelligence and machine learning in financial services: market developments and financial stability implications. https://www.fsb.org/wp-content/uploads/P011117.pdf (2017)
24. Tadros, *The Principle of Prevention of Harm under EU Ethics Guidelines for Trustworthy AI* (2011)
25. O.V. Sushkova, *Features of legal, ethical and social characteristics when testing a person's personal genome*. In the book: Genetic technologies and law during the formation of bioeconomics: monograph, otv. ed. A. A. Mokhov, O. V. Sushkova. M.: Prospect, 536 (2020)
26. O.V. Sushkova, Vlast 'zakona: scientific and practical journal **2(42)**, 99 (2020)
27. European Commission, Intrusive surveillance technologies would be considered ‘high risk’, 18 (2020)
28. O.A. Tarasenko, *Digital Banking in Russia* (§2). In the book: Digital economy: conceptual basic legal regulation of business in Russia: monograph, otv. ed. V.A. Laptev, O. A. Tarasenko. M.: Prospect, 351 (2020)
29. Deloitte, GDPR for funds. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/GDPR%20for%20Funds%20FINAL.pdf (2017a)
30. ESMA Technical advice to the Commission on MiFID II and MiFIR. https://www.esma.europa.eu/document/technical-advice-commission-mifid-ii-and-mifir (2014)
31. FCA Safe custody services and money laundering. https://www.fca.org.uk/firms/money-laundering/safe-custody-services (2017)