European Proceedings of
Social and Behavioural Sciences
EpSBS
www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.06.03.46

AMURCON 2020
International Scientific Conference

DEPLOYMENT OF AI IN BANKING: COMPARISON OF RUSSIAN AND SINGAPOREAN APPROACHES

Ella Gorian (a)*
*Corresponding author

(a) Vladivostok State University of Economics and Service, 41 Gogolya St., Vladivostok, Russia,
ella.gorian@gmail.com

Abstract

Artificial Intelligence technologies are widely accepted and are being used in banking globally. The main sphere of its implementation is the information security. The current situation of regulation of AI technologies in Russia and Singapore is being considered. Relevant government initiatives and regulatory instruments are characterized. The role of the financial regulators in processes of artificial intelligence deployment is being determined. A few general scientific (system-structural, formal-logical and hermeneutic methods) and special legal methods of cognition (comparative legal and formal-legal methods) are being used. The Russian approach to AI regulation put the public authorities in the centre of mechanism. In Russia as well as in Singapore the legal basis of AI deployment comprises numerous sector-oriented rules, but the special legal act on AI use is still absent. The same situation is in banking sector – only national financial regulators are responsible for development and implementation of regulations and standards in the sphere of informational security and AI use. But the Monetary Authority of Singapore is a step ahead of the Russian financial regulator after issuing the guideline on the use of AI and data analytics (FEAT Principles), which is being followed by financial and banking institutions. This instrument helps to ensure the unified approach within the industry and to minimise risks emerging from the use of AI.

Keywords: Artificial intelligence, information security, banking, Russia, Singapore

https://doi.org/10.15405/epsbs.2021.06.03.46
Corresponding Author: Ella Gorian
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Artificial intelligence technologies (AI technologies) are gaining popularity in banking and financial sectors. AI technologies are being used by the largest Russian national bank - Sberbank of Russia: AI approves more than 90% of consumer loans and over 50% of mortgage loans, as well as the issuance of 100% of credit cards. Since 2019 AI is an integral component of mobile application. The most discussed issues in Russian banking are the technologies for launching the financial products on the market; technologies for client remote verification and fraud protection; monetization of new paradigm of customer relations; digitalization of financial services; deployment of digital services in banking; the lack of solutions in b2b segment; cybersecurity, and new opportunities in the regulatory field. Singapore is a globally recognized leader in digitalization and implementation of artificial intelligence. In November 2014, Singapore launched a Smart Nation Singapore project aimed at digital integration of the society comprising digital economy, digital government and digital society. In 2017, four advanced technologies that will contribute to the development of the basic infrastructure of the digital economy have been identified: AI, cybersecurity, immersive media and the Internet of Things.

The use of AI technologies in retail banking services is a standard technological process, now it is a turn for investment banking. Such impressive results should not diminish the degree of attention to AI technologies: since they are a type of information technology, the security is the question that naturally emerge. In addition, the banking and financial sectors are a part of national critical information infrastructure, that makes them the priority target for cyber-attacks. Therefore, the issue of AI deployment and information security is relevant and essential for the development of a sustainable and effective cybersecurity mechanism.

Singapore is the largest international financial centre, therefore its experience in AI deployment in banking and financial organisations will influence the implementation of these technologies by other nations – the subjects of the international financial system. So the comparison of Russian and Singaporean models is important for studying the positive experience of the global financial centre and refining the Russian approach to AI deployment in banking sector.

2. Problem Statement

There are two different approaches in regulation of AI technologies implementation: regulatory (when a state prescribes the imperative regulations and controls the process of AI deployment) and self-regulatory (when a state envisages a certain framework of principles and expects both public and private sectors to participate in a rule-making process). Russia is following the regulatory approach: both the National Strategy for the Development of Artificial Intelligence and the National program “Digital Economy of the Russian Federation” entail the leading role of public authorities and national corporations in ensuring information security. Singapore, on the contrary, has envisaged the policies and projects aimed at the broadest involvement of private sector actors (pro-business approach).

3. Research Questions

The completion of a comparative study on deployment of artificial intelligence in banking requires the finding of answers to the certain research questions. First, the current regulation of Artificial Intelligence use in Russia and Singapore is to be characterised. Second, the relevant government initiatives and regulatory instruments are to be analysed. And third, the peculiarities of deployment of AI in banking sectors of the states are to be determined.

4. Purpose of the Study

Legal system of a state comprises the certain principles and methods of regulation. The approaches which are being used by the state reflect the model of communication of public and private actors. The purpose of the study is to identify the main features of Russian and Singaporean approaches to the regulation of artificial intelligence use in the banking and financial sectors.

5. Research Methods

In this study we will use the general methods (system structural, formal logical and hermeneutic ones) as well as the special legal methods of scientific knowledge (comparative legal and formal legal methods).

6. Findings

AI is being used in various spheres of life. Despite the potential consequences of such a widespread deployment of AI, that have been widely discussed by scholars and researchers (Hu et al., 2020; Lagioia & Sartor, 2020; Schwalbe & Wahl, 2020), there is a need for a legal definition of AI and its determination in legal relations. Despite the limitations imposed by the modern level of technology, computing power is growing exponentially (according to Moore's law the number of transistors in a dense integrated circuit doubles about every two years) and in ten years the mankind will have the computing power, that is two hundred times higher than the modern one, which, in turn, will lead to a corresponding increase in the capabilities of AI systems. All industries are trying to use the existing AI technologies to optimize and qualitatively develop processes. As a result, in perspective the market will be divided among those who have relied on the widest deployment of AI technologies.

Nowadays AI technologies are actively being used to ensure information security of the financial and banking sector covering the following areas: combating money laundering and fraud; aggregation of security data; monitoring of cyber threats and prevention of cyber-attacks. For example, the OpenMLEngine data processing software is operating to detect and prevent money laundering and fraud in 10 largest US banks. It is used to approve customers application and since its launch the number of approved applications has increased by 70% while the time spent on manual review has been reduced. Despite the increase in the number of users of banking services, the amount of fraudulent activities has decreased. The experts emphasize that the AI technologies aimed at detecting fraud and combating money laundering are the most popular now, and next 3-5 years the software products that detect fraud threats in real time will be developed and globally deployed in banking and financial institutions (Bharadwaj, 2019).

Russian approach. In Russia, the development and deployment of AI technologies have been regulated as a part of implementation of the National Technology Initiative in 2016 (hereafter NTI), although since 2014 AI has been proclaimed as one of the top priorities of national policy (Horian & Gorian, 2020). The "Artificial Intelligence" project as a part of NTI is being supervised by the Moscow Institute of Physics and Technology (MIPT). The MIPT's NTI Centre of competences has been formed uniting in consortium more than 20 scientific and educational institutions, partners from the industry and small innovative companies, including the largest national bank Sberbank as a representative of the banking sector. The NTI Centre of competences conduct a comprehensive development of the end-to-end technology "Artificial Intelligence". As for the banking sector, the outcome is the fundamentally new technologies for biometric identification of users through the analysis and intelligent processing of human reflex reactions - the development of technology and service for remote biometric identification based on the reflex reactions of a person to exciting stimuli designed to distrust the client device (for example, a smartphone) for verification of transactions during the banking and government service delivery.

Since 2019 the development of AI is a separate national strategy named National strategy of development of AI 2030, and it consolidates the principles of development and deployment of AI technologies, as well as it establishes the goals and main tasks for the development. The National strategy of development of AI 2030 contains the legal definition of AI and AI technologies: it defines the AI technologies through the open list of processes where AI can be deployed (after listing the most promising modern AI processes the wording "promising methods" of AI has been used to enforce the possibility of including the other technologies that may appear in the future according to the above mentioned Moore's law).

The National strategy of development of AI 2030 includes the main principles for the development and deployment of AI technologies (para. 19): a) protection of human rights and freedoms. AI deployment processes should comply with the protection of human rights and freedoms guaranteed by national and international rules, including the right to work. Individuals are guaranteed the opportunity to acquire knowledge and skills for successful adaptation to the digital economy; b) safety: the inadmissibility of using AI for the purpose of intentionally causing harm to individuals and legal entities. All risks of negative impact of AI technologies have to be prevented and minimized; c) transparency: the AI processes should be explainable including the process to obtaining the results. All users have an access to the information about the products and services using AI on non-discriminatory basis; d) technological sovereignty. The necessary level of independence of the Russian Federation in the field of AI is to be maintained, including the predominant use of domestic AI technologies and technological solutions developed on the basis of AI; e) the integrity of the innovation cycle. The close interaction of research, development and industry should be maintained; f) reasonable frugality. The existing measures aimed at the implementation of national policy in scientific, technical and other areas are the top priority on AI deployment; g) competitiveness support. The Russian entities involved in AI research, development and deployment processes are granted the freedom of market and anti-monopoly policies.

Among the objectives of AI development, two should be noted that are closely related to security in banking and financial sectors: development of the software based on the AI technologies (para. 24b) and the creation of an integrated regulatory system for public relations in the sphere of development and use of AI technologies (para. 24e). To fulfil these two objectives, the creation of an integrated security system is needed during the processes of creation, development, implementation and use of AI technologies (para. 25f). The responsible authority for security in financial and banking sector is a financial regulator. In Russia this function is entitled to the Bank of Russia, that regulates the activities of infrastructure projects (digital identification, instant money transfer system) and cyber security issues (Gorian, 2020). It should be noted that despite its high authoritative status the Bank of Russia is not involved in the work of the Centre of competence "Information Security" formed under the NTI. Such a situation does not correlate both with a rigid approach of legislator to financial system regulation (Alekseenko, 2019) and with the constitutional status of Russian financial regulator, and it disbalances the mentioned integrated security system.

To date there is no any specific instrument on AI deployment within information security system of banking and financial operations. The regulations of the Bank of Russia cover such aspects as protection of information systems, risk management and outsourcing. Although there are numerous legal acts which contain provisions to be applied to different aspects of AI deployment: on copyright and patent protection, on personal data protection, on information and cybersecurity, and on critical information infrastructure.

The biggest bank of Russia – Sberbank is a leader in innovations on AI development and deployment. Since 2019 it has been deployed in its business processes a platform for development, validation, and business monitoring of AI models - Sber.DS. This platform helps to deal with more than 2 thousands AI models being used by in front and middle office processes. It simplifies the process of checking the quality of models. The leading advantage of Sber.DS platform is the significant reduction of the extension costs and independence of any programming language.

Singaporean approach. In 2019 Singapore presented a Model AI Governance Framework 2019 (Model Framework) at the World Economic Forum in Davos (WEF). Its simplicity and relevance were the factors that inspired many international organizations to adopt and implement it in production processes. It was highly evaluated by the European Commission's High-Level Expert Group and the OECD Expert Group on AI. The Singapore Model Framework is one of five projects being implemented as part of the 2017 National AI Singapore Program and National Artificial Intelligence Strategy 2019.

AI technologies in Singapore are being deployed in transport and logistics, industry, finance, cybersecurity, etc. The Model Framework defines two high-level guiding principles that promote trust in AI and understanding of the use of AI technologies (para. 2.7): (1) clarity, transparency, and fairness. Organizations using AI in decision-making must ensure that the process is clear, transparent and fair. Although perfect explainability, transparency and fairness are impossible to attain, organizations should strive to ensure that their use or application of AI is undertaken in a manner that reflects the objectives of these principles as far as possible; (2) anthropocentric approach - AI solutions should be human-centred. As AI is used to empower human capabilities, the protection of people's interests (including their well-being and safety) must be a top priority when designing, developing and deploying AI solutions.

Walters and Coghlan emphasize that Singapore is implementing a more balanced approach towards AI governance on the basis of an accountability-based framework for discussing ethical, governance and consumer protection issues related to the commercial deployment of AI in a systematic and structured manner (Walters & Coghlan, 2019). The developed Model Framework possesses such unique characteristics: 1) principles-based approach: the Model Framework espouses a proper governance structure with clear responsibility assigned to individuals when deploying AI. A clear definition of roles and accountability - be they an algorithm engineer or a businessperson - is fundamental to ensure responsible deployment of AI. use cases; 2) collaborative approach – the industry and the government are working together as partners to come up with some of these measures and frameworks. The industry then applies it during the pilot stage and provides feedback to the Government; 3) practical approach - organisations are encouraged to participate in the pilot and provide feedback in order to improve the Model Framework; 4) global and international approach – the Model Framework is being promoted at the WEF and is considered as an example model by the WEF's Centre for the Fourth Industrial Revolution (C4IR); 5) business and objective approach - customers are put first, businesses are being simulated to be open und their operations to be explainable (Remolina & Seah, 2019).

AI technologies in Singapore are being regulated by legal provisions of specific acts to be applied to different aspects of AI deployment: the Copyright Act 1987, the Patent Act 1994, the Competition Act 2004 in relation to anti-competitive agreements and concerted actions supported by algorithms; Cybersecurity Act 2018 and the Protection from Online Falsehood and Manipulation Act 2019.

The Model Framework states (para. 2.13) that certain sectors of the economy (such as finance and banking, medicine and legal) may be regulated by existing sector-specific laws, regulations or guidelines. In particular, the Monetary Authority of Singapore has issued the Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, which should be used by financial operators while deploying AI technologies and data analytics in financial products and services.

By its legal validity, the FEAT Principles can be classified as a guideline, one of the instruments that is created by the Monetary Authority of Singapore as a financial regulator (Alekseenko, 2020). FEAT principles govern the conduct of financial operators: violation of such regulations is not a criminal offense and does not entail administrative sanctions, however, the degree of adherence to such guidelines affects the overall risk assessment for a financial operator.

One of the first financial operators that implemented the Model Framework and the FEAT Principles deploying the AI technology was the largest multinational bank in Southeast Asia - DBS Bank. It provides banking and financial services in 18 jurisdictions around the world, with over 100 branches in Singapore alone. To improve operational efficiency and the effectiveness of ongoing supervision for money laundering, DBS Bank has developed and successfully implemented an AI technology - Anti-Money Laundering (AML) Filter Model (AML-filter) to identify predictive indicators of suspicious transactions to reduce the number of false positives generated by the non-AI system, thereby reducing the number of alerts that require manual review.

DBS Bank determines the level of human participation in the processes of making AI decisions and ensures the responsible use of data by the AML Filter. The developers gained a complete and comprehensive understanding of the processes of data origin and triggers of transaction notifications, combined with the transparent calculation of the results generated by the AML Filter, which gave the bank the opportunity to explain the work of its AI technology and predict the risk rating.

To ensure the stability of the AML Filter, DBS Bank monitors the indicators monthly, for which the results of the training, testing and verification stages are used as a reference. Additionally, monthly and semi-annual checks are carried out by machine learning specialists. This extra precaution guarantees that any deviation from predefined thresholds is detected. In addition, the bank has implemented an internal control system to eliminate the risks associated with the use of the AML Filter, and developed an appropriate communication with stakeholders (both internal - senior management and board, and external - Monetary Authority of Singapore).

7. Conclusion

The Russian approach to AI regulation puts the state authorities in the centre of regulatory mechanism, although the Bank of Russia as a national financial regulator is excluded from the participation in the development of instruments in the field of AI deployment in information security. Despite the involvement of stakeholders from public and private sector into the National Technology Initiative, the state keeps the authoritative style of regulation. In Russia as well as in Singapore the legal basis of AI deployment comprises numerous sector-oriented rules, but the special legal act on AI use is still missing. The same situation is in banking sector – only national financial regulators are responsible for development and implementation of regulations and standards in the sphere of informational security and AI use. But the Monetary Authority of Singapore is a step ahead of the Russian financial regulator after issuing the guideline on the use of AI and data analytics (FEAT Principles), which is being followed by financial and banking institutions. This instrument helps to ensure the unified approach within the industry and to minimise risks emerging from the use of AI: due to its flexibility and lability this instrument allows, on the one hand, to standardize processes, and on the other - to ensure the rights of consumers of financial and banking services. Therefore the participation of the financial regulator in these processes is of a coordinating and integrating nature, which makes it possible to use the experience and ideas of financial institutions for further unification of approaches and standards for the use of AI technologies.

Acknowledgments

The reported study was funded by RFBR, project number 20-011-00454 "Ensuring the rights of investors in the banking and financial sectors in the context of the digitalization of the economy in the Russian Federation and the leading financial centres of East Asia: a comparative legal aspect".

References

Alekseenko, A. (2019). New Russian model BIT and the practice of investment arbitration. *Manchester Journal of International economic Law, 1*(16), 79-93.

Alekseenko, A. (2020). Russian approach to ICO regulation. *Revista Genero & Direito, 4*(9), 874-881.

Bharadwaj, R. (2019). *AI for Cybersecurity in Finance – Current Applications*. https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications/

Gorian, E. (2020). Genesis of Russian cyber security legal mechanism: an authentic or a trend alike model? In Denis B. Solovev (Ed.), *Smart Technologies and Innovations in Design for Control of*

Technological Processes and Objects: Proceeding of the International Science and Technology Conference "FarEastCon-2019" (pp. 937-949). Springer.

Horian, K., & Gorian, E. (2020). Information security ensuring in the financial sector as part of the implementation of the National Program "Data Economy Russia 2024". *Advances in Economics, Business and Management Research: Proceedings of the International Scientific Conference "Far East Con" (ISCFEC 2020), 128*, 635-644. https://doi.org/10.2991/aebmr.k.200312.091

Hu, Y., Jacob, J., Parker, G. J. M., Hawkes, D. J., Hurst, J. R., & Stoyanov, D. (2020). The challenges of deploying artificial intelligence models in a rapidly evolving pandemic. *Nature Machine Intelligence, 2*, 298-300.

Lagioia, F., & Sartor, G. (2020). AI Systems Under Criminal Law: A Legal Analysis and a Regulatory Perspective. *Philosophy & Technology, 33*, 433–465.

Remolina, L. N., & Seah, J. (2019). *How to address the AI Governance discussion? What can we learn from Singapore's AI strategy?* https://ink.library.smu.edu.sg/caidg/1

Schwalbe, N., & Wahl, B. (2020). Artificial intelligence and the future of global health. *The Lancet, 395* (10236), 1579-1586.

Walters, R., & Coghlan, M. (2019). Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy? *American Journal of Science, Engineering and Technology, 4*(4), 55-65.