

Using artificial intelligence to counter money laundering and terrorist financing

Katarzyna Cyrkun¹, Karolina Nastaj-Sałek², Rober Sito³, Henryk Noga⁴ and Wojciech Jaubiec⁵

¹Military University of Technology
Poland

²State Vocational University of prof. Stanisław Tarnowski in Tarnobrzeg
Poland

³Constantin the Philosopher University in Nitra
Slovakia

⁴University of the National Education Commission, Kraków
Poland

⁵Bielsko-Biala University of Applied Sciences
Poland

Abstract— The study aimed to understand the impact of artificial intelligence on the effectiveness of measures to prevent money laundering and terrorist financing in the financial sector. Research problems focused on identifying areas where AI can effectively improve preventive actions and on understanding the challenges associated with implementing this technology in the context of financial security. The aim of the work included an analysis of the prospects for the development of AI in activities to prevent money laundering and terrorism financing and an assessment of its impact on the effectiveness of preventive activities. The research hypothesis assumed that developed AI systems could increase the effectiveness of detecting illegal transactions and terrorist activities. The conclusions indicate that the development of AI is crucial for the effective fight against financial crime, but at the same time requires constant adaptation to the evolving threat environment. The message of the study suggests that investments in the development of AI in the financial sector are necessary to maintain security and effectively prevent financial crime.

Keywords— Artificial intelligence, money laundering, terrorism financing, machine learning, innovative technologies, security.

I. INTRODUCTION

In the face of the dynamic development of technology, the use of artificial intelligence (AI) is becoming a key tool in various fields, including combating financial crime, such as money laundering and terrorism financing. The aim of this article is to explore the role of artificial intelligence in the context of counteracting these phenomena, analyzing the potential benefits, and identifying challenges related to the implementation of AI in anti-money laundering (AML) and counter-terrorist financing (CTF) systems.

The research problem can be summarized in the question: will the use of artificial intelligence have an impact on contemporary challenges related to money laundering and terrorism financing? In the context of this problem, the effective use of modern technologies, especially artificial intelligence, in preventing and combating these forms of crime becomes a critical issue.

The research hypothesis of the article assumes that the effective implementation of artificial intelligence in AML and CTF systems can significantly improve the ability to detect and



prosecute money laundering and terrorist financing. It is assumed that AI, based on machine learning algorithms, can effectively analyze massive amounts of financial data, identifying patterns and several types of anomalies that may be difficult to detect using traditional methods.

Research methods include a thorough analysis of scientific literature and case studies of implemented IS implementations in AML and CTF systems. Innovative approaches and tools based on artificial intelligence that have the potential to have a revolutionary impact on combating money laundering and terrorist financing will also be presented.

As technologies evolve at a rapid pace, reviewing these issues from the perspective of using artificial intelligence in the field of financial security becomes crucial to understanding how modern tools can be effectively used in the fight against financial crime. Money laundering and terrorist financing constitute a global threat, having a serious impact on the stability of economies and the security of societies (Turing, 2009).

II. ARTIFICIAL INTELLIGENCE IN THE FINANCIAL SECTOR

Before analyzing the role of artificial intelligence in counteracting these phenomena, it is worth understanding the theoretical foundations in more detail. Money laundering is the process of legalizing funds obtained illegally, often by transforming them into apparent, legal sources. It works like the so-called washing dirty money to cover up its illegal origins. It is often a multi-stage process, including various financial transactions, aimed at the so-called covering up traces (Dalvinder, 2014).

Terrorist financing, in turn, is the provision of financial resources or their equivalent to support terrorist activities. It may include providing funds for training terrorists, purchasing weapons or financing terrorist propaganda. This is an activity that aims to support organizations or individuals involved in acts of terrorism.

Criminals use a variety of money laundering techniques to make money more difficult to track. One common practice is to divide large sums of money into smaller transactions, which makes it easier to camouflage them. Other methods include investing in real estate, art, or businesses, which allows you to transfer funds to different assets (Hanafi, 2010)

Money laundering and terrorism financing generate a few negative effects. At the social level, they lead to distortion of economic competition, an increase in crime, and a loss of trust in financial institutions. The economic effects include destabilization of financial systems and loss of capital. On the security front, these consequences can be devastating. Terrorist financing enables extremist groups to obtain funds to pursue goals that threaten public order as well as the stability of societies. Moreover, laundered funds can be used to purchase weapons or carry out attacks, which increases the risk to national security (Hendriyetty & Grewal, 2017)

Understanding these fundamentals is the key to developing effective countermeasure strategies. The analysis of money

laundering and terrorist financing mechanisms is an extremely important step towards developing tools that will allow for the effective identification, monitoring and combating of these pathologies in the context of the global financial scene.

In the face of the growing threat of money laundering, financial institutions around the world are looking for modern tools that will allow for more effective combating of this practice. Artificial intelligence in this context is emerging as a key tool that can not only identify money laundering patterns, but also adapt to the evolving strategies of criminals. Below, an analysis of the role of AI in combating money laundering will be presented (Stylec-Szromek, 2018).

One of the most important areas in which AI can revolutionize the fight against money laundering is the analysis of very large financial data sets. Traditional methods are often limited in scale and complexity of the data analyzed. AI, using advanced machine learning algorithms, can process huge amounts of information, identifying subtle patterns that may indicate this type of activity.

In the context of combating money laundering, AI can be used to continuously learn from new data. Machine learning algorithms can analyze customers' financial behavior, identifying unusual transactions or suspicious patterns. As new data is collected, these systems become more and more precise in recognizing irregularities. It can be said that these systems, along with new data, acquire more and more possibilities (Hetemi, Merovci, & Gulhan, 2018)

Artificial intelligence allows automatic detection of transactions that may indicate money laundering attempts. Algorithms can assess the risk associated with a given transaction based on many factors - such as the transaction amount, location, frequency, or participants of a given transaction. This enables quick response to potential cases of participation in such illegal activities.

AI can also play an extremely key role in analyzing customer behavior. By monitoring and analyzing customer interactions with financial services, artificial intelligence systems can identify unusual patterns that may suggest money laundering attempts. This approach is based on the ability of AI to understand the context of the transaction, as well as build a comprehensive picture of customers' financial behavior.

With the growing popularity of blockchain technology, AI can also be used to monitor transactions in networks based on this technology. By analyzing distributed ledgers, AI can identify suspicious transactions and track the flow of funds through the blockchain network, which makes money laundering much more difficult.

The conclusions indicate that artificial intelligence is becoming a key element in combating money laundering. Its ability to analyze huge data sets, continuous learning and automatic detection of suspicious transactions makes AI an indispensable tool for financial institutions that strive to effectively counteract this phenomenon. The implementation of modern systems not only significantly increases the efficiency of operations, but also enables adaptation to the constantly changing landscape of money laundering.

III. THE USE OF ARTIFICIAL INTELLIGENCE IN COUNTERACTING MONEY LAUNDERING AND TERRORISM FINANCING

In the face of the growing threat from terrorism, effective tools to combat the financing of terrorist activities are becoming a priority for financial institutions and law enforcement agencies. In this context, artificial intelligence presents itself as a powerful tool, offering innovative methods of analyzing and identifying suspicious transactions. The implementation of AI in counterterrorism financing systems promises a revolution in the way financial sources of support for terrorist activities are identified and eliminated (Gao & Ye, 2007)

Artificial intelligence, especially in the context of machine learning, allows for a very deep analysis of many variables related to financial transactions. The use of advanced algorithms allows for the identification of patterns that may indicate potential attempts to finance terrorism. It is also crucial to monitor unusual, unusual transactions, which allows for quick detection and response to potential irregularities (Płoszajski, 2016).

The use of AI enables more effective detection of sources of terrorist financing. Algorithms analyze not only the transactions themselves, but also the connections between various financial entities. Thanks to this, it is possible to identify financial patterns that may suggest hidden channels for transferring funds for terrorist purposes.

Traditional methods of monitoring transactions may be insufficient in the face of dynamically developing money laundering techniques. AI allows you to monitor transactions in real time - which increases efficiency in identifying potentially dangerous operations. AI-based systems can analyze large sets of data in a very short time, enabling extremely quick responses to changing patterns of terrorist financing.

Despite promising prospects, the implementation of AI in combating terrorist financing is not without challenges. Issues related to data privacy protection, continuous improvement of algorithms and ensuring access to current financial data constitute significant challenges in this area. It is also necessary to consider ethical aspects to avoid abuses as well as violations of citizens' rights (Dubber, Pasquale & Das 2020).

In striving to effectively combat the financing of terrorism, artificial intelligence can be a powerful tool that can significantly help increase the effectiveness of actions taken by financial institutions and law enforcement agencies. However, as important as developing technology is maintaining a balance between the effectiveness of actions and compliance with individual rights and ethical norms (Hagendorff, 2020).

The implementation of artificial intelligence in anti-money laundering and anti-terrorist financing systems opens new perspectives for financial institutions in the effective identification and elimination of illegal activities.

One of the key areas of AI application in AML and CTF systems is the analysis of customer behavior. Machine learning algorithms analyze customer transactions, considering their history, preferences, and characteristic behavioral patterns. Based on this data, AI systems can identify unusual activities that may suggest attempts at money laundering or terrorist

financing.

An example could be a situation where a customer who usually makes small local transactions suddenly conducts a large transaction with a sanctioned country. The AI system, analyzing this context, can automatically classify the transaction as suspicious and report it for further analysis.

Big Data analysis is becoming a key tool in combating money laundering. AI systems, using advanced data processing algorithms, can analyze huge amounts of information in real time. An example of practical implementation is monitoring transactions on a global scale, as well as identifying patterns that indicate potential irregularities.

Artificial intelligence can be effectively used to identify subtle patterns of money laundering that may escape traditional analysis methods. Machine learning algorithms can identify complex transaction patterns that are characteristic of money laundering. For example, the AI system can detect a situation in which large sums of money are divided into smaller transactions to avoid suspicion (Rojszczak, 2020).

AI implementation also enables automation of the process of reporting suspicious transactions to the appropriate law enforcement authorities. Algorithms can automatically generate reports based on established criteria and forward them to law enforcement agencies. This effectively speeds up the response to potential threats and improves cooperation with regulatory authorities (Huang & Rust, 2018)

AI systems can effectively identify connections between various transactions, which is crucial in the context of combating money laundering and terrorist financing. For example, if multiple transactions appear unrelated, AI can discover hidden connections between them, suggesting complex criminal activity.

The dynamic nature of money laundering and terrorist financing requires flexible systems that can adapt to the evolving strategies of criminals. AI, using machine learning, can constantly improve its algorithms based on new data and detect new, previously unknown patterns.

The lessons from these practical examples suggest that implementing artificial intelligence in AML and CTF systems has the potential to revolutionize the way financial institutions counter money laundering and terrorist financing. The effectiveness of AI results from its ability to analyze large amounts of data, quickly respond to unusual situations and adapt to a changing environment. The implementation of these technologies is therefore becoming a key element of the strategy to counteract money laundering and terrorism financing.

IV. AND LIMITATIONS

The implementation of artificial intelligence in counteracting threats brings several challenges that need to be addressed effectively. Despite the potential benefits that AI can bring to these areas, there are some difficulties that may impact the effectiveness of these systems. The main challenges related to the implementation of AI in the fight against money laundering

and terrorist financing will be presented below.

The money laundering and terrorist financing environment is extremely complex and dynamic. Criminals are constantly adapting their tactics to avoid detection, which poses a challenge for AI systems. Continuous monitoring is necessary, as well as updating algorithms to keep up with new ways of operating criminals.

The diversity of money laundering schemes makes identifying suspicious transactions more difficult. Criminals use various methods, such as dividing transactions into smaller amounts, using the so-called "junk companies" or the use of new technologies. AI must be advanced enough to recognize these different patterns and adapt to them.

Processing large amounts of data to identify suspicious transactions may lead to a breach of customer privacy. When implementing AI, financial institutions must balance operational efficiency with respect for data privacy. It is necessary to apply appropriate data protection mechanisms and comply with privacy regulations.

Introducing AI into existing AML and CTF systems poses integration challenges. Financial institutions often have complex and extensive system structures that may be difficult to modernize. The need to efficiently connect SI with existing systems requires careful planning and adaptation to the specificity of a given organization.

The effective use of AI systems requires appropriate training of staff, both in the use of these systems and in understanding their role in the process of counteracting money laundering and terrorism financing. Employee education is a key element of success to avoid interpretation errors and maximize the potential of AI (Dignum, 2019).

The introduction of AI into financial systems makes them a potential target for cyber attacks. Advanced security measures are required to protect AI systems from unauthorized access, hacker attacks, and data theft.

In the context of global financial markets, cross-border crime poses a serious challenge. AI systems must be able to cooperate and exchange information between different jurisdictions to effectively combat money laundering and terrorist financing on an international scale.

In the face of these challenges, financial institutions and law enforcement agencies must approach the implementation of artificial intelligence with full understanding and special preparation. These activities require inter-sectoral cooperation, investment in technology development and constant monitoring and updating of these systems. As technology progresses, the effective use of AI may bring revolutionary changes in the fight against money laundering and terrorism financing (Brynjolfsson, McAfee, 2015).

perspectives and creates several opportunities for financial institutions and regulatory authorities. Below, we will discuss the prospects for the development of AI in the context of AML and CTF and outline the future that may lie ahead for this area.

The prospects for the development of deep learning in transaction analysis are broad. Algorithms based on this technology can be excellent at identifying unusual patterns, which is crucial in detecting suspicious financial operations. The evolution of these algorithms may lead to even more effective tools to combat money laundering (Gadre-Patwardhan, Katdare & Joshi, 2016).

The development of AI enables further automation of decision-making processes in AML and CTF. Systems based on artificial intelligence can make instant decisions based on the analysis of large amounts of data, which shortens the response time to potential threats. Automation can also reduce the workload on employees and increase operational efficiency.

Anomaly detection systems are a key element in anti-money laundering. The development of AI may lead to more sophisticated and dynamic tools that can recognize even subtle changes in transaction behavior. This, in turn, allows for more effective identification of potential threats.

The development prospects of AI also include its use in the prevention of financial crime. Algorithms can be used to analyze data from various sources, including social media, to detect potential criminal activities early. This proactive approach can prevent illegal activities before they begin.

The prospects for the development of AI in AML and CTF also include more advanced mechanisms for integrating data sets at a global level. Collaboration between countries and financial institutions can lead to the creation of more comprehensive models that consider global patterns and trends.

The development of AI requires a simultaneous focus on aspects related to cybersecurity. As the role of AI in the financial sector increases, it becomes an attractive target for cybercriminals. The evolution of security strategies and technologies is necessary to maintain the integrity of systems (Sastry, 2019).

The prospects for AI development also include improving user interaction. Systems can become more intuitive, making the work of analysts, as well as employees responsible for AML and CTF, easier. Implementing tools that facilitate interaction can increase the effectiveness of activities and reduce human errors.

As technology advances, AI is becoming a key tool in combating financial crime. However, alongside the benefits, institutions must diligently monitor and adapt their systems to meet the dynamic challenges and threats associated with the future development of this technology. The effective use of AI in the AML/CTF area will require flexibility, innovation, and close cross-sector cooperation.

V. PROSPECTS FOR THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN COUNTERACTING MONEY LAUNDERING AND TERRORISM FINANCING

The development of artificial intelligence opens new

VI. PRACTICAL USE OF ARTIFICIAL INTELLIGENCE IN COUNTERACTING MONEY LAUNDERING AND TERRORISM FINANCING

This section will discuss specific examples of AI applications in financial institutions and law enforcement agencies, presenting the tools, technologies and strategies used to analyze data, identify patterns, and effectively combat criminal activities in the fields of finance and national security.

Palantir Technologies is an American company specializing in data analysis and artificial intelligence. Its platform, Palantir Gotham, is widely used in the national security, counterterrorism, and anti-money laundering sectors. Palantir Gotham allows you to integrate data from a variety of sources, such as government databases, social media information, financial transactions, and more.

Palantir Gotham uses advanced data analytics technologies, including machine learning algorithms, to identify subtle patterns that may indicate terrorist activity or money laundering. The system enables analysts to access rich data sets, which helps them quickly respond to potential threats and suspicious transactions.

In the case of combating money laundering, Palantir Gotham can analyze large-scale financial transactions, identifying irregularities and irregularities. The system also enables tracking of financial flows on a global scale, which is crucial in combating money laundering at an international level.

Palantir Technologies cooperates with both government agencies and the private sector, providing analytical tools that allow for the effective use of the potential of data to counteract threats related to terrorism and money laundering. However, due to the nature of specific counterterrorism activities, details about specific Palantir Gotham implementations are often treated as confidential.

SAS Institute is a global leader in data analytics, and their Anti-Money Laundering (AML) solutions are widely used in the financial sector. SAS's artificial intelligence-based AML systems offer comprehensive tools to identify, monitor and counteract money laundering and terrorist financing.

One of the key elements of the SAS AML system is the use of advanced machine learning technologies. These algorithms analyze large amounts of financial data, identifying unusual transaction patterns that may indicate illegal activity. The system is capable of learning on the fly, adapting to changing criminal strategies.

SAS AML enables banks and financial institutions to monitor transactions in real time and identify potential threats. By analyzing customer data, the system can automatically detect suspicious transactions, considering various factors such as transaction history, customer profile or risk related to specific geographical areas.

In addition, SAS AML allows you to automatically generate compliance reports with legal regulations. The system is adapted to various regulations and standards, which helps financial institutions meet the requirements of anti-money laundering law. Analytical modules also enable deeper data analysis, which supports investigations and participation in

investigations conducted by law enforcement agencies.

In practice, financial institutions such as banks and money transfer companies use SAS AML systems to effectively counter money laundering and terrorist financing while meeting regulatory obligations (Teichmann, & Falker, 2020)

In turn, IBM Watson Financial Services is a segment of IBM that offers innovative solutions based on artificial intelligence aimed at improving financial security and counteracting money laundering and terrorist financing. As part of its services, IBM Watson Financial Services provides several tools and analytical platforms that use advanced technologies to identify and monitor illegal financial activity.

One of the key elements of the company's offer is the IBM Financial Crimes Insights platform, which integrates data from various sources, such as financial transactions, customer information, social media data, and information from open sources. This platform uses powerful machine learning algorithms, analyzing large amounts of data in real time.

IBM Financial Crimes Insights enables you to identify irregularities in transaction behavior, detect patterns related to money laundering, and identify potential links to terrorist activity. This system can automatically generate warnings and reports for financial analysts, which speeds up the response to potential threats.

Additionally, IBM Watson Financial Services also offers risk management and regulatory compliance (RegTech) tools. These systems help financial institutions meet increasing regulatory requirements by automating reporting, monitoring, and risk management processes.

IBM's finance and security activities are widely used by financial institutions around the world, and their innovative approach to the use of artificial intelligence supports effective measures to counteract money laundering and terrorist financing.

As technology evolves, artificial intelligence is becoming a key tool in combating money laundering and terrorist financing. Companies, financial institutions, and law enforcement agencies around the world use advanced algorithms and AI systems to analyze data, identify transaction patterns and effectively respond to possible threats. The examples presented, such as SAS Anti-Money Laundering systems or the Palantir Gotham platform, show how modern technologies support financial security efforts. Integrating AI into anti-money laundering strategies is becoming an essential element of effective protection against today's dynamic financial and terrorist threats.

VII. CONCLUSIONS

In summarizing the issue of the use of artificial intelligence in counteracting money laundering and terrorist financing, it is necessary to emphasize the significant progress that this technology brings for the financial sector. The aim of the work was to thoroughly examine the prospects for the development of artificial intelligence in the context of counteracting money laundering and terrorism financing. The aim was also to

indicate what new opportunities and challenges arise in connection with the implementation of this technology in processes related to financial security.

The solution to the research problem involved identifying areas in which artificial intelligence can effectively support financial institutions in combating financial crime. The adopted research hypothesis concerned the potential of using artificial intelligence to improve AML and CTF systems and increase the effectiveness of preventive actions.

Confirmation of the research hypothesis is reflected in the analysis of the prospects for IS development in AML and CTF. Artificial intelligence is becoming an irreplaceable tool in identifying and combating illegal financial activities. Process automation, the use of deep learning and the analysis of large data sets enable more effective prevention and response to possible threats.

The conclusions from the presented study indicate that the development of artificial intelligence brings real benefits to the financial sector in the context of security. However, with the increased effectiveness of AML and CTF systems, new challenges are emerging related to cybersecurity, the ethics of using algorithms, and the need to constantly adapt to the changing landscape of financial crime (Anderson, M. & Anderson, L. S. 2007).

The article constitutes a basis for further research on this dynamically developing area. It is necessary to closely monitor technological progress and adapt the strategy for counteracting money laundering and terrorism financing to the latest achievements of artificial intelligence. Ultimately, the effectiveness of the fight against financial crime will depend on the ability of institutions to intelligently use and improve artificial intelligence-based tools.

VIII. REFERENCES

- Anderson, M., Anderson, L. S. (2007). Machine Ethics: Creating an Ethical Intelligent Agent. *AI Magazine*, No. 28(4)
- Brynjolfsson, E., McAfee, A. (2015). *Drugi wiek maszyn. Praca, postęp i dobrobyt w czasach genialnych technologii*, MT Biznes, Warszawa/
- Dalvinder, S. G. (2014). A Critical Conceptual Analysis of Definitions of Artificial Intelligence as Applicable to Computer Engineering, *IOSR Journal of Computer Engineering*, No. 16(2).
- Dignum, V. (2019). *Responsible Artificial Intelligence. How to develop and use AI in a responsible way*. Springer, Dubber.
- Dubber M. D., Pasquale, F., Das, S. (2020). *The Oxford Handbook of Ethics of AI*. Oxford University Press, Oxford.
- Gadre-Patwardhan, S., Katdare, V.V., Joshi, M.R. (2016). A Review of Artificially Intelligent Applications in the Financial Domain, eds. C. Dunis, P. Middleton, A. Karathanasopolous, K. Theofilatos, *Artificial Intelligence in Financial Markets. New Developments in Quantitative Trading and Investment*, Palgrave Macmillan, London.
- Gao, Z. and Ye, M. (2007) A Framework for Data Mining-Based Anti-Money Laundering Research. *Journal of Money Laundering Control*, No. 10.
- Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds and Machines*, No. 30.
- Hanafi, A. (2010) The Dynamic Aspects of Criminal Act and Criminal Liability in Money Laundering Practices, *Jurnal Hukum Ius Quia Iustum*, No. 17.

Hendriyetty, N. and Grewal, B.S. (2017) Macroeconomics of Money Laundering: Effects and Measurements, *Journal of Financial Crime*, No. 24.

Hetemi, A., Merovci, S. and Gulhan, O. (2018) Consequences of Money Laundering on Economic Growth—The Case of Kosovo and Its Trade Partners. *Acta Universitatis Danubius*, No. 14.

Huang, M.H. and Rust, R.T. (2018) Artificial Intelligence in Service. *Journal of Service Research*, No. 21.

Płoszajski, P. (2016). Czy nadszedł zmierzch monopolu człowieka na inteligencję? O maszynach myślących jak ludzie i ludziach myślących jak maszyny, *Oficyna Wydawnicza SGH, Warszawa*.

Płoszajski, P. (2016). *Spółeczna odpowiedzialność technologii*, Oficyna Wydawnicza SGH, Warszawa.

Rojszczak, M. (2020). Sztuczna inteligencja w innowacjach finansowych – aspekty prawne i regulacyjne, *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, No. 2(9).

Sastry, V. V. L. N. (2019). *Artificial Intelligence in Financial Services and Banking Industry*, Blue Diamond Publishing, Shabbir.

Stylec-Szromek, P. (2018). Sztuczna inteligencja – prawo, odpowiedzialność, etyka, *Organizacja i Zarządzanie*, No. 123.

Teichmann, F.M. and Falker, M.C. (2020) Money Laundering through Consulting Companies. *Journal of Financial Regulation and Compliance*, No. 28

Turing, A.M. (2009). *Computing Machinery and Intelligence*, eds. Computer, R. Epstein, G. Roberts, G. Beber, *Parsing the Turing Test. Philosophical and Methodological Issues in the Quest for the Thinking*, Springle, Dordrecht.