Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

Application of Machine Learning in Detection and Prevention of Money Laundering with Cryptocurrencies

Mojtaba Goodarzi[1] , Mahdi Khaghani Isfahani[2*], Mohammad Ali Kanani[3]

[1] Department of Humanities, Criminal Law and Criminology, Kish International Branch, Islamic Azad University, Kish Island, Iran
mgoodarzi359@gmail.com
[2] Department of Humanities, Criminal Law and Criminology, The Institute for Research and Development in Humanities (SAMT), Tehran, Iran khaghani@samt.ac.ir
[3] Department of Humanities, Criminal Law and Criminology, Roodhen Branch, Islamic Azad University, Tehran, Iran
dr.kanani110@gmail.com

Abstract: Money laundering, as a critical challenge for financial systems, has become increasingly complex with the advent of cryptocurrencies. Features such as anonymity and the ability for rapid, cross-border transfers have rendered cryptocurrencies attractive tools for illicit activities, including money laundering. Machine learning, as an advanced technological approach, offers promising capabilities for detecting suspicious patterns and preventing money laundering within decentralized financial systems. However, the efficacy of this approach hinges on the formulation of a sophisticated criminal policy framework that leverages the opportunities offered by cryptocurrencies while mitigating associated risks. This study, employing a descriptive-analytical methodology, examines legal challenges such as the absence of comprehensive and harmonized global regulations, regulatory issues like the lack of international standards for monitoring cryptocurrency transactions, and technical difficulties, including the complexity and volume of transaction data and user anonymity. The findings underscore the necessity of international legal cooperation and harmonized criminal policy strategies to combat money laundering in the cryptocurrency domain. Machine learning models, while holding significant potential for enhancing oversight and crime prevention, require a robust legal and regulatory framework to realize their full potential in addressing financial crimes within this emerging technological landscape.
Keywords: machine learning, cryptocurrency transactions, money laundering, criminal policy.

JCDSA, Vol. 2, No. 3, Autumn 2024	Online ISSN: 2981-1295	Journal Homepage: https://sanad.iau.ir/en/Journal/jcdsa
Received: 2024-08-24	Accepted: 2024-11-20	Published: 2024-12-20

CITATION

Goodarzi, M., et. al., *" Application of Machine Learning in Detection and Prevention of Money Laundering with Cryptocurrencies "*, Journal of Circuits, Data and Systems Analysis (JCDSA), Vol. 2, No. 3, pp. 1-15, 2024.

DOI: 00.00000/0000

* Corresponding author

Extended Abstract

1- Introduction

Money laundering has long been one of the most pressing challenges for global financial systems, and the advent of cryptocurrencies has introduced new layers of complexity. Due to features such as anonymity, decentralization, and rapid cross-border transfers, cryptocurrencies have become attractive tools for facilitating illegal financial activities, particularly money laundering. In traditional systems, money laundering involved complex schemes like using shell companies and fake identities, but cryptocurrencies have added new dimensions by leveraging blockchain technology and peer-to-peer transactions.

Machine learning (ML), as a subset of artificial intelligence, presents a promising solution for identifying and preventing money laundering activities within the cryptocurrency ecosystem. ML algorithms can detect suspicious patterns that might go unnoticed through traditional monitoring systems. However, the implementation of machine learning in financial regulation, particularly in cryptocurrency transactions, presents legal, regulatory, and technical challenges. These challenges are further compounded by the absence of comprehensive international legal frameworks governing cryptocurrency transactions, which makes cross-border enforcement and cooperation difficult. This paper investigates the potential of machine learning to combat money laundering in cryptocurrency transactions, while focusing on the regulatory, legal, and technical obstacles that hinder its effectiveness, particularly in the context of Iran's financial system.

2- Methodology

This study adopts a descriptive-analytical research methodology, utilizing both qualitative content analysis and a comparative approach. The analysis focuses on the intersection of cryptocurrency, machine learning, and anti-money laundering (AML) regulations. It examines legal texts, regulatory standards, and technical documentation to explore the challenges and solutions associated with the implementation of machine learning in monitoring cryptocurrency transactions. Furthermore, the paper compares international frameworks, such as those provided by the Financial Action Task Force (FATF), with Iran's legal and regulatory system, highlighting gaps and opportunities for improvement.

The research also investigates case studies of how ML algorithms such as Random Forests, XGBoost, Graph Convolutional Networks (GCNs), and Deep Neural Networks have been applied in real-world scenarios to detect money laundering activities. These case studies provide insight into the strengths and limitations of ML in the cryptocurrency space, especially in light of the vast amount of data and the anonymity provided by certain cryptocurrencies.

3- Results and discussion

The results show that machine learning models, when applied correctly, can significantly enhance the accuracy and efficiency of monitoring cryptocurrency transactions. Key advantages include:

- High accuracy: Algorithms like neural networks and GCNs detect hidden patterns in large datasets that manual or traditional rule-based systems miss.
- Real-time monitoring: ML allows for immediate detection of suspicious behaviors, which is essential given the fast-paced nature of cryptocurrency transactions.
- Adaptive learning: ML models continuously improve, which is vital for combating constantly evolving money laundering tactics.
- However, several challenges need to be addressed, particularly in Iran, including:
- Legal gaps: Iran's AML laws do not explicitly address ML or cryptocurrency-specific challenges, and the lack of global standards complicates cross-border enforcement.

Technical limitations: ML requires substantial computational resources and expertise, which are often limited in developing economies like Iran.

Regulatory barriers: Many Iranian cryptocurrency exchanges lack clear oversight, making it difficult to implement effective ML-based monitoring systems.

4- Conclusion

This study highlights the critical role machine learning can play in combating money laundering in cryptocurrencies. Technologies like Random Forests and GCNs show promise but require a supportive legal and regulatory framework to be effective. Key recommendations for Iran include:

- Developing clear legal frameworks: Policymakers must create regulations for using ML in financial monitoring and cryptocurrency transactions, aligned with global standards.
- Strengthening technical infrastructure: Investments in computational resources, expertise, and data quality are essential for implementing ML-based systems.
- Promoting international cooperation: Iran should engage in global discussions on AML regulations, especially related to cryptocurrencies, to align its policies with international norms.

In conclusion, while ML offers substantial promise in combating money laundering in cryptocurrency transactions, legal, technical, and regulatory reforms are essential for realizing its full potential in Iran's financial system. By addressing these challenges, Iran can harness the power of ML to enhance its AML capabilities and protect its financial system in the increasingly digital and decentralized global economy.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

کاربست یادگیری ماشینی در کشف و پیشگیری از پولشویی با رمزارزها

مجتبی گودرزی[1]، مهدی خاقانی اصفهانی[2*]، محمدعلی کنعانی تیکمه داش[3]

۱- گروه علوم انسانی، حقوق جزا و جرم شناسی، واحد بین الملل کیش، دانشگاه آزاد اسلامی، جزیره کیش، ایران (mgoodarzi359@gmail.com)
۲- گروه علوم انسانی، حقوق جزا و جرم شناسی، پژوهشکده تحقیق و توسعه علوم انسانی (سمت)، تهران، ایران (khaghani@samt.ac.ir)
۳- گروه علوم انسانی، حقوق جزا و جرم شناسی، واحد رودهن، دانشگاه آزاد اسلامی، تهران، ایران (dr.kanani110@gmail.com)

چکیده: پولشویی، به‌عنوان یکی از چالش‌های کلیدی نظام‌های مالی، با ظهور رمزارزها ابعاد پیچیده‌تری یافته است. ویژگی‌هایی نظیر ناشناس بودن و انتقال سریع و فرامرزی رمزارزها، آن‌ها را به ابزاری جذاب برای جرایمی همچون پولشویی تبدیل کرده است. یادگیری ماشینی، به‌عنوان یک ابزار پیشرفته، قابلیت شناسایی الگوهای مشکوک و پیشگیری از پولشویی در سیستم‌های مالی غیرمتمرکز را دارد. با این حال، موفقیت این فناوری مستلزم تدوین سیاست جنایی هوشمندانه است که بتواند هم از مزایای رمزارز بهره‌برداری کند و هم مخاطرات آن را کاهش دهد. این پژوهش، با روش توصیفی-تحلیلی، به بررسی چالش‌های حقوقی نظیر نبود قوانین جامع و جهانی، چالش‌های مقرراتی مانند فقدان استانداردهای بین‌المللی برای نظارت بر تراکنش‌های رمزارزی، و چالش‌های فنی از جمله پیچیدگی و حجم بالای داده‌ها و ناشناس بودن کاربران می‌پردازد. تأکید بر همکاری بین‌المللی و هماهنگی سیاست‌های جنایی برای مقابله با پولشویی در حوزه رمزارزها ضروری است. یافته‌ها نشان می‌دهند که مدل‌های یادگیری ماشینی می‌توانند نقش مهمی در بهبود نظارت و پیشگیری از جرایم مالی مرتبط با رمزارزها ایفا کنند، اما این امر مستلزم چارچوب‌های قانونی و نظارتی مناسب است.

واژه های کلیدی: یادگیری ماشینی، تراکنش‌های رمزارزی ، پولشویی، سیاست جنایی

نوع مقاله: مروری
تاریخ ارسال مقاله: ۱۴۰۳/۰۶/۰۳ تاریخ پذیرش مقاله: ۱۴۰۳/۰۸/۳۰ تاریخ چاپ مقاله: ۱۴۰۳/۰۹/۳۰
DOI: 00.00000/0000

۱- مقدمه

با ظهور رمزارزها به‌عنوان یکی از نوآوری‌های مهم فناوری در دهه‌های اخیر، فرصت‌ها و چالش‌های جدیدی برای نظام‌های مالی جهانی به وجود آمده است. در حالی که رمزارزهایی مانند بیت‌کوین و اتریوم به‌عنوان ابزارهایی برای تسهیل تراکنش‌های مالی و بهبود سطح مبادلات اقتصادی مورد استقبال قرار گرفته‌اند؛ به دلیل ویژگی‌های خاص خود مانند ناشناس بودن، عدم وابستگی به نهادهای مرکزی و قابلیت انتقال سریع و فرامرزی، به‌طور هم‌زمان به ابزاری مطلوب برای فعالیت‌های غیرقانونی از جمله پولشویی تبدیل شده‌اند. تنها در اوایل سال ۱۳۹۹، ده‌ها پرونده سنگین در شعب مجتمع تخصصی رسیدگی به جرایم اقتصادی مفتوح شده که حجم قابل‌توجهی از آنها اتهامات پولشویی است [۱]. پولشویی در بستر رمزارزها با پیچیدگی بیشتری نسبت به پولشویی سنّتی مواجه است؛ چراکه رهگیری و شناسایی تراکنش‌های مالی در این حوزه به مراتب دشوارتر از سیستم‌های مالی سنتی است. از سوی دیگر، قدرت و گستردگی رمزارزها به‌طور بالقوه امکان توسعه و اجرای سیاست‌های مالی و جنایی هوشمندانه‌تری را فراهم می‌آورد که بتوانند هم‌زمان با تسهیل تجارت قانونی، از سوءاستفاده‌های مالی آن جلوگیری کنند. اهمیت موضوع در این است که در مواجهه با این چالش‌ها، سیاست‌گذاران، نهادهای نظارتی و مجریان قانون نیازمند ابزارها و رویکردهای نوینی برای شناسایی و پیشگیری از پولشویی در فضای رمزارزها هستند. یکی از این ابزارهای نوین، یادگیری ماشینی است که به‌عنوان بخشی از هوش مصنوعی، قابلیت‌های فراوانی در تحلیل حجم عظیمی از داده‌ها، تراکنش‌ها و شناسایی الگوهای مشکوک دارد. استفاده از یادگیری ماشینی می‌تواند به‌طور قابل‌توجهی فرآیند شناسایی و پیشگیری از پولشویی در تراکنش‌های رمزارزی را بهبود بخشد و به نهادهای نظارتی این امکان را بدهد که با دقت و سرعت بیشتری فعالیت‌های مشکوک را شناسایی کرده و ارتباط آن را با اتخاذ یک سیاست جنایی مطلوب در قبال جرایمی نظیر پولشویی در حوزه رمزارزها تحلیل کنند. فقدان سیاست جنایی در این زمینه، از این حیث ضرورت ویژه به چاره‌جویی می‌طلبد که به‌رغم نپیوستن ایران به کنوانسیون‌های پالرمو و تأمین مالی تروریسم و تبعاً عدم لزوم رعایت مقررات آنها در خصوص ارزهای رمزنگاری‌شده، در صورتی که ایران تمایلی به پیوستن به این نهادها در آینده هم نداشته باشد، باز باید مقررات مربوط به

* نویسنده مسئول

پولشویی از طریق ارزهای رمزنگاری‌شده را اجرا کند و مؤسسات ارائه‌دهنده خدمات این ارزها را ملزم به اجرای این قوانین سازد [۲].

ایران نمی‌تواند به‌تنهایی و بدون همکاری‌های بین‌المللی در راستای مبارزه با پولشویی گام بردارد. مبارزه با پولشویی در ایران داستان شگفت‌انگیز و غم‌باری است که هم اصل محرمانگی را نادیده می‌گیرد و هم اصل شفافیت را به قربانگاه می‌برد [۳]. ایران، نه دارای سیاست جنایی مدل زرد (احتیاطی) نسبت به رمزارزها است، نه پیرو سیاست جنایی مدل قرمز (تحریمیِ سزاگرا) و نه هم‌داستان با سیاست جنایی مدل سبز (روادار و موافق با رمزارزها و ناجرم‌انگار) می‌باشد [۴]. در واقع، سیاست جنایی خاصی در قبال رمزارزها و جرایم ناشی یا همبسته با آنها در کشور وجود ندارد. بخشنامه مورخ بهمن‌ماه سال ۱۳۹۷ از سوی معاونت فناوری‌های نوین اداره نظام‌های پرداخت بانک مرکزی با عنوان «الزامات و ضوابط حوزه رمزارزها»، در جهت اعتبارسنجی و بیان ویژگی‌های این ارزها مقرر شده است و به لحاظ تهی‌بودن از مقررات‌گذاری محتوایی و شکلی، به معنای دقیق تقنین، از مقررات خاص، صرفاً به‌سان گزارشی از ویژگی‌های این ارزها است. در این مقاله تلاش شده است تا نقش یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی مورد بررسی قرار گیرد. این امر به‌ویژه از آن جهت اهمیت دارد که مقالات و تحقیقات قبلی عمدتاً به مباحث فنی و فناوری پرداخته‌اند و کمتر به تحلیل‌های حقوقی، سیاست‌گذاری و قانونی در این زمینه توجه کرده‌اند. بنابراین، این پژوهش تلاش دارد تا با ارائه دیدگاهی چندجانبه، گامی در جهت تکمیل ادبیات موجود در این حوزه بردارد و به تبیین ضرورت توجه به سیاست جنایی هوشمندانه‌ای که می‌تواند از سوءاستفاده‌های مالی در حوزه رمزارزها جلوگیری کند، کمک نماید. مسئله اصلی این پژوهش به چالش‌های حقوقی، مقرراتی و فنی استفاده از یادگیری ماشینی برای شناسایی پولشویی در تراکنش‌های رمزارزی بازمی‌گردد. از یک سو، نبود قوانین جامع و استانداردهای بین‌المللی مشخص برای مقابله با پولشویی در حوزه رمزارزها و، از سوی دیگر، پیچیدگی فنی تحلیل حجم بالای داده‌های ناشناس در این تراکنش‌ها، ضرورت تدوین سیاست‌های جنایی هوشمندانه و استفاده مؤثر از فناوری‌های نوین را پررنگ‌تر کرده است. این پژوهش به دنبال پاسخ‌گویی به این چالش‌ها و ارائه راهکارهایی برای بهره‌برداری از یادگیری ماشینی در شناسایی و پیشگیری از پولشویی است. ذیل پرسش اصلی مزبور، سؤالاتی قابل طرح است که این مقاله در کندوکاو پیرامون آن‌هاست:

۱ .چگونه می‌توان قوانین و مقررات حقوقی را برای استفاده از یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی بهبود بخشید؟

۲ .چه راهکارهای فنی برای مقابله با چالش‌های تحلیل داده‌های رمزارزی از طریق یادگیری ماشینی وجود دارد؟

۳ .چگونه سیاست‌های جنایی هوشمندانه‌ای می‌توان تدوین کرد که از فناوری یادگیری ماشینی در مقابله با پولشویی در حوزه رمزارزها بهره ببرند؟

۲- پیشینه پژوهش

خلیلی پاجی در کتاب ارزهای مجازی؛ جهانی‌شدن بزهکاری و سیاست جنایی که در نشر میزان به چاپ دوم رسیده است، جهانی‌شدن بعضی جلوه‌های بزهکاریِ مالی ارتکابی توسط مرتکبان چندملیتی به‌طور سازمان‌یافته یا در قالب گروه‌های جنایی ساختارمند را تشریح کرده و تدابیر تقنینی، قضایی و اجرایی نظام‌های سیاست جنایی در پیشگیری و مجازات جرایم رمزارزها را تبیین کرده است. در مطالعه‌ای که در «مجله کنترل پولشویی» منتشر شد، به بررسی کاربرد یادگیری ماشینی[1] برای شناسایی و مقابله با پولشویی در صرافی‌های ارزهای دیجیتال پرداختند. این تحقیق نشان داد که روش‌های فعلی برای شناسایی پولشویی ناکارآمد بوده و نیاز به بهبود دارند؛ به‌ویژه در زمینه ارزهای دیجیتال. با مقایسه چهار الگوریتم یادگیری نظارت‌شده، این مطالعه تأکید کرد که الگوریتم درخت تصمیم به‌طور خاص برای شناسایی تراکنش‌های مشکوک در صرافی‌های رمزارزی مناسب‌تر است. نتایج این پژوهش همچنین بر اهمیت توسعه فناوری‌های نوین برای مبارزه مؤثرتر با پولشویی تأکید دارد.

در پژوهشی دیگر با عنوان «تجزیه و تحلیل کلان‌داده برای پیش‌بینی رفتارهای مالی بر اساس یادگیری ماشین» نشان دادند که استفاده از الگوریتم‌های یادگیری ماشین مانند الگوریتم گرگ خاکستری می‌تولند در پیش‌بینی بحران‌های مالی و تحلیل رفتارهای اقتصادی مؤثر باشد. این مطالعه با بهره‌گیری از داده‌های ۱۳۶ شرکت بین سال‌های ۱۳۹۴ تا ۱۳۹۷ نشان داد که مدل‌های یادگیری ماشین در ترکیب با کلان‌داده می‌توانند به پیش‌بینی دقیق‌تر و سریع‌تر ورشکستگی و بحران‌های مالی کمک کنند. در مطالعه‌ای دیگر به بررسی استفاده از تکنیک‌های یادگیری ماشین و یادگیری عمیق در شناسایی و مقابله با پولشویی پرداختند. این تحقیق بر ضرورت توسعه تکنیک‌های مؤثر برای شناسایی تراکنش‌های مشکوک، به‌ویژه در حوزه رمزارزها، تأکید دارد. در این پژوهش، از مدل‌های یادگیری عمیق و یادگیری ماشین شامل شبکه عصبی عمیق[2]، جنگل تصادفی[3]، الگوریتم K نزدیک ترین همسایه[4] و بیز ساده[5] با استفاده از مجموعه‌داده بیت کوین بیضوی[6] بهره گرفته شده است. در یکی از تحقیق‌ها، به بررسی چالش‌های قانونی و مقرراتی مرتبط با استفاده از یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی پرداختند. این مطالعه نشان داد که اگرچه الگوریتم‌های یادگیری ماشینی پتانسیل بالایی در این زمینه دارند، اما همچنان نیاز به تدوین چارچوب‌های قانونی و مقرراتی مناسب برای حمایت از استفاده گسترده از این فناوری‌ها وجود

[1] MashineLearning
[2] Deep Neural Networks
[3] Random Forest
[4] K-Nearest Neighbors
[5] Naive Bayes Classifiers
[6] Elliptic Bitcoin

دارد. این تحقیق بر اهمیت همکاری بین‌المللی برای تدوین سیاست‌های جنایی مناسب در مقابله با پولشویی تأکید کرد.

در یک مطالعه دیگر، پیشرفت‌های اخیر در به‌کارگیری الگوریتم‌های یادگیری ماشینی و تکنیک‌های داده‌کاوی برای شناسایی ناهنجاری‌ها و پولشویی در تراکنش‌های رمزارزی بررسی شده است. این پژوهش بر نظارت بر تراکنش‌ها در شبکه‌های بلاک‌چین متمرکز است و نشان می‌دهد که ترکیب روش‌های یادگیری ماشینی با تکنیک‌های تحلیل گراف می‌تواند به بهبود دقت و کارایی سیستم‌های نظارتی منجر شود. در این مطالعه، اهمیت کیفیت داده‌ها برای آموزش مدل‌های یادگیری ماشینی به‌طور ویژه مورد تأکید قرار گرفته و چالش‌ها و مسیرهای تحقیقاتی آینده در این حوزه بررسی شده است. در مقاله‌ای با عنوان «واکاوی نقش هوش مصنوعی در چرخه سیاست‌گذاری عمومی؛ رویکرد فراترکیب»، به بررسی ابعاد مختلف کاربرد هوش مصنوعی در سیاست‌گذاری عمومی پرداختند. آن‌ها دریافتند که هوش مصنوعی می‌تواند با تحلیل کلان‌داده‌ها و شناسایی الگوهای موجود، به اولویت‌بندی مسائل و تدوین سیاست‌های مبتنی بر شواهد کمک کند. با این حال، چالش‌های اخلاقی و امنیتی، از جمله موانع اصلی در استفاده گسترده از این فناوری در این حوزه به شمار می‌روند.

تحقیقات گذشته نشان می‌دهد که استفاده از یادگیری ماشینی در شناسایی و پیشگیری از پولشویی توسط رمزارزها به سرعت در حال توسعه است و پیشرفت‌های فنی مهمی در این زمینه رخ داده است. اما این مطالعات بیشتر بر جنبه‌های فنی تمرکز داشته و کمتر به ابعاد حقوقی و سیاست‌گذاری مرتبط با این فناوری‌ها پرداخته‌اند. این مقاله با هدف پر کردن این خلأ، بر ارتباط میان سیاست جنایی و استفاده از یادگیری ماشینی در مقابله با پولشویی توسط رمزارزها تأکید دارد و نشان می‌دهد که رویکردی چندجانبه، شامل توجه به قوانین و سیاست‌گذاری، ضروری است. در این پژوهش، نقش یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی و ارتباط آن با سیاست جنایی در پیشگیری از این جرم مورد بررسی قرار گرفته است. برای این منظور، از روش‌های پژوهش توصیفی و تحلیل محتوا استفاده شده است. این روش‌ها، با تکیه بر منابع کتابخانه‌ای و پایگاه‌های اطلاعاتی معتبر علمی، امکان تحلیل جامع و دقیق موضوع را فراهم می‌کنند. این پژوهش با اتخاذ رویکردی بین‌رشته‌ای، به ترکیب تحلیل‌های حقوقی و فنی پرداخته است. تأثیرات و کاربردهای فناوری یادگیری ماشینی در زمینه شناسایی پولشویی، نه‌تنها از منظر فنی بلکه از دیدگاه حقوقی و سیاست‌گذاری نیز مورد بررسی قرار گرفته است. کارایی و قابلیت‌های این فناوری در پیشگیری از پولشویی، چالش‌ها و فرصت‌های موجود در این زمینه و تأثیرات آن بر سیاست‌های جنایی نیز ارزیابی شده‌اند. در این بین، چارچوب‌های قانونی و سیاست‌های جنایی مرتبط با استفاده از فناوری‌های نوین در مبارزه با پولشویی تحلیل شده و خلأها و چالش‌های موجود در قوانین و مقررات جاری شناسایی و پیشنهاداتی برای بهبود و تقویت سیاست‌های جنایی ارائه شده است. با وجود تلاش برای انجام یک پژوهش جامع و دقیق، برخی محدودیت‌ها در این مطالعه وجود داشته است. محدودیت‌هایی همچون دسترسی محدود به برخی منابع، تغییرات سریع در حوزه رمزارزها و یادگیری ماشینی که ممکن است برخی از یافته‌ها را تحت تأثیر قرار دهد، و تنوع قوانین و مقررات در سطح بین‌المللی که تحلیل جامع و یکپارچه را دشوار می‌سازد، از جمله چالش‌های این پژوهش بوده است.

۳- فناوری‌های شناسایی و پیشگیری وضعی از پولشویی

فناوری‌های مختلفی، به‌ویژه در دهه‌های اخیر، به‌منظور شناسایی و جلوگیری از پولشویی به‌کار گرفته شده‌اند. این فناوری‌ها شامل ابزارهای تحلیل داده، تحلیل بلاکچین، و الگوریتم‌های یادگیری ماشینی هستند که به‌طور خاص برای شناسایی الگوهای پولشویی طراحی شده‌اند. با ظهور رمزارزها و پیچیدگی‌های جدیدی که این فناوری به‌وجود آورده است، استفاده از این فناوری‌ها ضروری شده است. در ایران، با توجه به اجرای قانون مبارزه با پولشویی مصوب ۱۳۸۶ و اصلاحات آن در سال ۱۳۹۷، استفاده از فناوری‌های پیشرفته مانند یادگیری ماشینی و تحلیل بلاکچین به‌عنوان بخشی از رویکردهای نظارتی جدید مورد توجه قرار گرفته است؛ اما نبود زیرساخت‌های فنی کافی و چارچوب‌های قانونی صریح در این زمینه همچنان چالش‌های زیادی برای اجرایی شدن کامل این فناوری‌ها به همراه دارد.

۳-۱- تحلیل داده‌ها

ابزارهای تحلیل داده‌ها، به‌ویژه در نهادهای مالی و نظارتی، به‌منظور شناسایی الگوهای غیرقانونی و فعالیت‌های مشکوک به پولشویی می‌توانند بسیار مؤثر باشند. این ابزارها با استفاده از تکنیک‌هایی مانند تحلیل روند، شبیه‌سازی، و ارزیابی ریسک، به شناسایی و پیشگیری از فعالیت‌های غیرقانونی کمک می‌کنند. این ابزارها قادر به پردازش و تحلیل حجم‌های وسیع از داده‌های تراکنش هستند و می‌توانند الگوهای غیرعادی و غیرقانونی را شناسایی کنند [۵]. در ایران، پیاده‌سازی این سیستم‌ها به زیرساخت‌های پیشرفته‌تر و آموزش پرسنل نظارتی نیاز دارد تا داده‌های تراکنش‌های مالی و رمزارزی را به‌طور دقیق‌تر تحلیل کرده و الگوهای مشکوک را به‌موقع شناسایی کرد. برای مثال، با بهره‌گیری از این فناوری‌ها در نهادهای نظارتی ایران، می‌توان به کشف و پیگیری تراکنش‌های مشکوک در بانک‌ها و صرافی‌های فعال در حوزه رمزارزها پرداخت که به‌طور فعالی در فضای دیجیتال کار می‌کنند و احتمال سوءاستفاده از آن‌ها برای پولشویی وجود دارد.

۳-۲- تحلیل بلاکچین

با توجه به ویژگی‌های خاص رمزارزها و استفاده از بلاکچین به‌عنوان یک دفترکل توزیع‌شده که تراکنش‌ها را به‌صورت غیرقابل تغییر ثبت می‌کند، تحلیل بلاکچین به یکی از ابزارهای کلیدی در مبارزه با پولشویی تبدیل شده است. با استفاده از ابزارهای تحلیل بلاکچین، نهادهای نظارتی می‌توانند به‌طور دقیق‌تر تراکنش‌های مالی را نظارت کرده و مسیر پولشویی را ردیابی کنند [۶]. در ایران، با توجه به رشد سریع بازار

رمزارزها و فعالیت‌های اقتصادی که به‌طور رسمی و غیررسمی در این حوزه انجام می‌شود، استفاده از فناوری تحلیل بلاکچین می‌تواند به شناسایی تغییرات غیرعادی در تراکنش‌ها و ردیابی وجوه مشکوک کمک شایانی کند. با توجه به تأکید قوانین مبارزه با پولشویی ایران بر استفاده از فناوری‌های نوین، تحلیل بلاکچین می‌تواند به ایجاد شفافیت بیشتر و مقابله با فعالیت‌های غیرقانونی مرتبط با پولشویی در حوزه رمزارزها کمک کند.

۳-۳- الگوریتم‌های یادگیری ماشینی

یادگیری ماشینی یکی از پیشرفته‌ترین فناوری‌ها در شناسایی و پیشگیری از پولشویی است که در ایران نیز قابلیت بهره‌برداری بالایی دارد. الگوریتم‌های یادگیری ماشینی قادر به شناسایی الگوهای پیچیده و پیش‌بینی فعالیت‌های غیرقانونی بر اساس داده‌های تاریخی و تحلیل‌های پیشرفته هستند. در ایران، نهادهای نظارتی و مالی با به‌کارگیری این الگوریتم‌ها می‌توانند تراکنش‌های مشکوک را به‌طور خودکار شناسایی کرده و از پولشویی در مراحل اولیه جلوگیری کنند. با وجود این، به‌کارگیری این فناوری‌ها نیازمند توسعه زیرساخت‌های فنی و آموزشی است که تاکنون به‌طور کامل محقق نشده است. به‌طور خاص، الگوریتم‌های پیشرفته‌ای مانند «جنگل تصادفی»[1] و «ایکس‌جی‌بوست»[2] می‌توانند به شناسایی الگوهای پنهان در تراکنش‌های مالی کمک کنند؛ در بسیاری از موارد، این تراکنش‌ها مربوط به پولشویی از طریق رمزارزها هستند[۷]. در ایران، با توجه به محدودیت‌های قانونی و نظارتی، استفاده از این فناوری‌ها می‌تواند نقش مهمی در تقویت سیستم‌های نظارتی کشور ایفا کند و شناسایی دقیق‌تر و سریع‌تری از فعالیت‌های مشکوک را امکان‌پذیر کند.

۴- ارتباط یادگیری ماشینی با هوش مصنوعی

یادگیری ماشینی به‌عنوان یکی از زیرشاخه‌های کلیدی هوش مصنوعی، نقش بسیار مهمی در پیشرفت و توسعه این حوزه ایفا می‌کند. هوش مصنوعی به‌طور کلی به تلاش‌های علمی و مهندسی اطلاق می‌شود که هدف آن ساخت سیستم‌هایی است که قادر به انجام وظایف انسانی مانند تفکر، یادگیری و تصمیم‌گیری باشند. یادگیری ماشینی به‌عنوان یکی از ابزارهای اصلی برای دستیابی به اهداف هوش مصنوعی شناخته می‌شود. این فناوری به‌ویژه در زمینه‌های مختلفی از جمله "پردازش زبان طبیعی"[3]، "بینایی کامپیوتری"[4] و رباتیک به طور گسترده‌ای استفاده می‌شود [۸]. در ایران، توسعه یادگیری ماشینی به‌عنوان بخشی از فناوری‌های هوش مصنوعی برای شناسایی و پیشگیری از جرایمی نظیر پولشویی از طریق رمزارزها به‌ویژه در نهادهای نظارتی و مالی کشور، مورد نیاز است. اما چالش‌هایی چون کمبود زیرساخت‌های فنی، نبود قوانین جامع و مشکلات آموزش نیروی انسانی همچنان مانعی برای بهره‌برداری کامل از این فناوری‌ها به شمار می‌روند.

۴-۱- پردازش زبان طبیعی

پردازش زبان طبیعی یکی از زیرمجموعه‌های هوش مصنوعی است که به تحلیل و درک زبان انسانی می‌پردازد. به‌عنوان مثال، تحلیل متون مبادلات و چت‌ها در پلتفرم‌های رمزارزی می‌تواند به شناسایی فعالیت‌های مشکوک و الگوهای پولشویی کمک کند [۹]. در ایران، با توجه به توسعه روزافزون پلتفرم‌های رمزارزی و استفاده از زبان فارسی در تراکنش‌ها و مکالمات مرتبط، بهره‌گیری از پردازش زبان طبیعی می‌تواند به تحلیل متون و مکالمات مربوط به تراکنش‌های مالی کمک کند. این فناوری، به‌ویژه در شناسایی فعالیت‌های مشکوک و پولشویی در پیام‌ها و مکالمات مرتبط با تراکنش‌های رمزارزی، برای نهادهای نظارتی ایران ارزش زیادی دارد؛ به‌خصوص در شرایطی که تحلیل و رصد مکالمات و متون رمزارزی با چالش‌هایی همراه است.

۴-۲- بینایی کامپیوتری

بینایی کامپیوتری به پردازش و تحلیل تصاویر و ویدئوها می‌پردازد. هرچند کاربرد مستقیم آن در پولشویی ممکن است کمتر باشد، در ایران می‌تواند در شناسایی و تحلیل مستندات و مدارک مرتبط با تراکنش‌های رمزارزی مفید باشد [۱۰]. استفاده از این فناوری در تحلیل اسناد و مدارکی که در تراکنش‌های مشکوک ارائه می‌شود، می‌تواند برای نهادهای اجرایی و قضایی ایران کارآمد باشد و به بهبود شفافیت و دقت در ردیابی پولشویی کمک کند.

۴-۳- یادگیری عمیق

یادگیری عمیق[5]، یکی از تکنیک‌های پیشرفته یادگیری ماشینی، به‌ویژه در تحلیل داده‌های پیچیده و حجیم به‌کار می‌رود. این فناوری می‌تواند به‌طور مؤثری به بهبود دقت و کارایی سیستم‌های نظارتی کمک کند و به شناسایی سریع‌تر و مؤثرتر فعالیت‌های غیرقانونی در تراکنش‌های مالی دیجیتال منجر شود [۱۱]. در ایران، با توجه به رشد سریع تراکنش‌های رمزارزی و نبود شفافیت در برخی تراکنش‌ها، استفاده از یادگیری عمیق می‌تواند به شناسایی الگوهای غیرمعمول در تراکنش‌ها و پیش‌بینی فعالیت‌های مشکوک کمک کند. مدل‌های شبکه عصبی عمیق، به‌ویژه شبکه‌های پیچشی و بازگشتی، قادر به تحلیل داده‌های پیچیده و بزرگ‌مقیاس هستند و می‌توانند به‌طور دقیق‌تری به شناسایی پولشویی در ایران بپردازند. در شرایطی که تراکنش‌های مشکوک در

---

[1] Random Forest

[2] XGBoost (Extreme Gradient Boosting) یک الگوریتم یادگیری ماشینی است که برای شناسایی و پیشگیری از فعالیت‌های پولشویی در تراکنش‌های رمزارزی کاربرد دارد. این الگوریتم با ایجاد مدل‌های تقویتی قدرتمند و دقیق، می‌تواند الگوهای پیچیده و مخفی در داده‌ها را شناسایی کرده و به تحلیل‌های دقیق‌تر و مؤثرتری در حوزه سیاست جنایی و مبارزه با جرایم مالی کمک کند. XGBoost به‌ویژه در تحلیل داده‌های بزرگ و پیچیده مفید است و بهبود عملکرد نظارتی و اجرایی را در این زمینه ممکن می‌سازد.

[3] Natural Language Processing

[4] Computer Vision

[5] Deep Learning

بستر رمزارزها به دلیل ناشناس بودن و پیچیدگی بالایی که دارند، شناسایی آن‌ها دشوار است، یادگیری عمیق می‌تواند به حل این مشکلات کمک کند.

۴-۴- انواع الگوریتم‌های یادگیری ماشینی و کاربردهای آن‌ها

در ایران، استفاده از انواع مختلف الگوریتم‌های یادگیری ماشینی برای مقابله با جرایم مالی، نظیر پولشویی، می‌تواند بسیار مؤثر باشد. با توجه به اینکه سیستم‌های مالی و نظارتی کشور با حجم بالای تراکنش‌ها روبه‌رو هستند و بخشی از آن‌ها ممکن است به فعالیت‌های مشکوک و غیرقانونی مرتبط باشند، الگوریتم‌های یادگیری ماشینی، مانند الگوریتم‌های یادگیری تحت نظارت و بدون نظارت، می‌توانند به شناسایی الگوهای مشکوک و پیشگیری از وقوع جرایم مالی کمک کنند. این الگوریتم‌ها به‌طور کلی به سه دسته اصلی تقسیم می‌شوند:

۴-۴-۱- الگوریتم‌های یادگیری تحت نظارت

الگوریتم‌های یادگیری تحت نظارت[1] یکی از اصلی‌ترین تکنیک‌های یادگیری ماشینی هستند که برای تحلیل داده‌های برچسب‌خورده مورد استفاده قرار می‌گیرند. این الگوریتم‌ها بر اساس داده‌هایی که شامل ورودی‌ها و خروجی‌های مشخص هستند، آموزش می‌بینند تا قادر به پیش‌بینی یا طبقه‌بندی داده‌های جدید شوند [۱۲]. الگوریتم‌های یادگیری تحت نظارت می‌توانند به تحلیل داده‌های تراکنش‌های رمزارزی در ایران کمک کنند. این الگوریتم‌ها با استفاده از داده‌های تاریخی و آموزش بر روی آن‌ها، قادرند تراکنش‌های جدید را تحلیل کرده و تراکنش‌های مشکوک را شناسایی کنند. به‌ویژه در شرایطی که ایران به دنبال ارتقای سیستم‌های نظارتی مالی است، این الگوریتم‌ها می‌توانند در شناسایی و گزارش‌دهی تراکنش‌های غیرقانونی به مقامات نظارتی نقش مهمی ایفا کنند.

۴-۴-۲- الگوریتم‌های یادگیری بدون نظارت

الگوریتم‌های یادگیری بدون نظارت[2] یکی از مهم‌ترین ابزارهای یادگیری ماشینی هستند که برای تحلیل داده‌های بدون برچسب و کشف ساختارهای پنهان در داده‌ها طراحی شده‌اند. برخلاف الگوریتم‌های یادگیری تحت نظارت که با داده‌های برچسب‌خورده کار می‌کنند، این الگوریتم‌ها به دنبال شناسایی الگوها و ساختارهای داخلی داده‌ها بدون نیاز به اطلاعات قبلی در مورد دسته‌بندی داده‌ها هستند. در زمینه پولشویی از طریق رمزارزها، این الگوریتم‌ها می‌توانند به شناسایی الگوهای غیرمعمول و فعالیت‌های مشکوک کمک کنند. برخی از مهم‌ترین الگوریتم‌های یادگیری بدون نظارت به شرح زیر است:

۴-۴-۳- تحلیل مؤلفه‌های اصلی

تحلیل مؤلفه‌های اصلی[3] یکی از تکنیک‌های کاهش ابعاد داده است که به شناسایی ویژگی‌های اصلی و مهم در داده‌های چندبعدی کمک می‌کند. این تکنیک می‌تواند در ایران برای شناسایی الگوهای غیرمعمول و کاهش پیچیدگی داده‌های تراکنش‌های رمزارزی مؤثر باشد. این ابزار با فشرده‌سازی داده‌ها و استخراج ویژگی‌های اصلی، به مقامات نظارتی کمک می‌کند تا با دقت بیشتری تراکنش‌های مشکوک را شناسایی کنند. با توجه به حجم بالای داده‌های مالی و تراکنش‌های انجام‌شده در ایران، استفاده از تحلیل مؤلفه‌های اصلی می‌تواند به شناسایی دقیق‌تر در زمینه پولشویی از طریق رمزارزها کمک شایانی کند.

۵- بسترمندی رمزارزها برای ارتکاب پولشویی

پولشویی به مجموعه‌ای از فرایندها و اقداماتی اطلاق می‌شود که به‌منظور تبدیل درآمدهای حاصل از فعالیت‌های غیرقانونی به منابع مالی که به نظر قانونی و مشروع می‌آیند، به‌کار گرفته می‌شود. این فرایند معمولاً شامل چندین مرحله است که هر یک به نوعی به پنهان‌سازی و توجیه منشأ واقعی وجوه کمک می‌کند. با ظهور فناوری‌های جدید و رمزارزها، این فرایند پیچیده‌تر و متنوع‌تر شده است. در پولشویی دیجیتال، رمزارزها و فناوری بلاکچین به‌ویژه به دلیل ویژگی‌هایی نظیر ناشناسی نسبی و عدم نیاز به واسطه‌های سنتی، زمینه‌های جدیدی برای پولشویی فراهم کرده‌اند. این شامل استفاده از صرافی‌های رمزارز، انتقال وجوه بین کیف‌پول‌های دیجیتال و استفاده از فناوری‌های مخفی‌کننده تراکنش‌ها مانند میکسرها و توکن‌های ناشناس است. پولشویی از طریق رمزارزها به‌ویژه به دلیل ویژگی‌های خاص این فناوری‌ها، نیازمند تکنیک‌های پیچیده و نوآورانه است که به بررسی و تحلیل دقیق الگوهای تراکنش‌ها و فعالیت‌های مشکوک در شبکه‌های غیرمتمرکز می‌پردازد. در ایران، با توجه به رشد سریع استفاده از رمزارزها و نبود قوانین جامع در این زمینه، استفاده از این فناوری برای پولشویی به یکی از نگرانی‌های اصلی نهادهای نظارتی تبدیل شده است. نهادهای نظارتی کشور باید زیرساخت‌ها و چارچوب‌های قانونی جدیدی را برای مقابله با پولشویی از طریق رمزارزها تدوین کنند.

۵-۱- ویژگی‌های رمزارزها و سختی‌های پیشگیری وضعی از آنها در مهار پولشویی

رمزارزها ویژگی‌های خاصی دارند که آن‌ها را به ابزارهایی جذاب برای پول‌شویان تبدیل می‌کند. در ایران، چالش‌های خاصی برای مقابله با پولشویی از طریق رمزارزها وجود دارد که شامل ضعف زیرساخت‌های نظارتی، نبود چارچوب قانونی صریح و همچنین مشکلات بین‌المللی مرتبط با تحریم‌ها و محدودیت‌های جهانی است. ویژگی‌هایی مانند

[1] Supervised Learning Algorithms.
[2] Unsupervised Learning Algorithms.
[3] Principal Component Analysis

ناشناس بودن، غیرمتمرکز بودن و حجم بالای تراکنش‌ها، شناسایی هویت کاربران و ردیابی منشأ وجوه غیرقانونی را دشوار و نظارت بر تراکنش‌ها را پیچیده‌تر می‌سازند. به‌ویژه، ناشناس بودن تراکنش‌ها و عدم وجود نهاد مرکزی، غیرمتمرکز بودن بلاکچین و امکان انجام تراکنش‌های جهانی بدون واسطه‌های بانکی سنتی، مشکلات زیادی برای نهادهای نظارتی به‌وجود آورده است. حجم بالای تراکنش‌ها نیز به پول‌شویان کمک می‌کند تا به‌سرعت و در مقیاس بزرگ وجوه را جابجا کنند. این چالش‌ها نیاز به سیاست‌گذاری‌ها، رهیافت‌های جدید و فناوری‌های نوین مانند الگوریتم‌های یادگیری ماشینی و ابزارهای تحلیل بلاکچین را ضروری می‌کند. در حالی که قانون مبارزه با پولشویی ایران مصوب ۱۳۸۶ و اصلاحات آن در سال ۱۳۹۷ بر اهمیت استفاده از فناوری‌های نوین تأکید کرده‌اند، اما همچنان چالش‌های فنی و نظارتی برای مقابله با پولشویی از طریق رمزارزها وجود دارد. نهادهای نظارتی ایران باید از فناوری‌های پیشرفته مانند یادگیری ماشینی و تحلیل بلاکچین برای افزایش دقت در نظارت بر تراکنش‌های رمزارزی استفاده کنند و با تقویت همکاری‌های بین‌المللی، به شناسایی بهتر جرایم مالی بپردازند.

۵-۲- روش‌های متداول پولشویی در فضای رمزارز

پولشویی در فضای رمزارز از تکنیک‌ها و روش‌های متنوعی بهره می‌برد که برای پنهان‌سازی منشأ وجوه غیرقانونی طراحی شده‌اند. در ایران، عدم وجود زیرساخت‌های نظارتی کافی و ضعف در اجرای دقیق قوانین ضد پولشویی[1] و شناخت مشتری[2] در برخی صرافی‌های داخلی، این مشکل را تشدید می‌کند. روش‌هایی که پول‌شویان از آن‌ها بهره می‌برند، شامل تراکنش‌های پیچیده و استفاده از رمزارزهای با حریم خصوصی بالاست برخی از این روش‌ها عبارتند از:

۵-۲-۱- تراکنش‌های پیچیده

پول‌شویان از تراکنش‌های پیچیده برای پنهان‌سازی منشأ پول‌های غیرقانونی استفاده می‌کنند. در ایران، با توجه به رشد استفاده از رمزارزها و نبود نهادهای نظارتی تخصصی در این زمینه، تراکنش‌های مکرر و پیچیده رمزارزها بین صرافی‌های داخلی و خارجی می‌تواند به راحتی وجوه غیرقانونی را در شبکه رمزارزی پنهان کند. نهادهای نظارتی کشور باید با بهره‌گیری از فناوری‌های نوین مانند الگوریتم‌های یادگیری ماشینی و همکاری با نهادهای بین‌المللی، تراکنش‌های پیچیده را به‌طور دقیق‌تر شناسایی کنند و مانع از گسترش فعالیت‌های پولشویی شوند [۱۳].

۵-۲-۲- صرافی‌های رمزارز با ضوابط ضعیف

در ایران، صرافی‌های رمزارز با ضوابط ضعیف، به یکی از چالش‌های اصلی در مقابله با پولشویی تبدیل شده‌اند. برخی از این صرافی‌ها به‌دلیل عدم تمایل یا توانایی در اجرای دقیق قوانین ضد پولشویی و شناخت مشتری، به محلی جذاب برای پول‌شویان تبدیل شده‌اند. این صرافی‌ها امکان انجام تراکنش‌های ناشناس و غیرقانونی را فراهم می‌کنند و می‌توانند به‌راحتی وجوه غیرقانونی را تبدیل و انتقال دهند. برای مقابله با این چالش، نهادهای نظارتی ایران باید مقررات جدیدی را برای نظارت دقیق‌تر بر صرافی‌های رمزارز داخلی وضع کنند و از فناوری‌هایی مانند یادگیری ماشینی برای شناسایی فعالیت‌های مشکوک استفاده کنند.

۵-۲-۳- استفاده از رمزارزهای با حریم خصوصی بالا

استفاده از رمزارزهای با حریم خصوصی بالا یکی از روش‌های پیشرفته پولشویی در فضای رمزارزها محسوب می‌شود. برخی رمزارزها به دلیل ویژگی‌های قوی در حفظ حریم خصوصی، جذابیت ویژه‌ای برای پول‌شویان دارند. این رمزارزها از تکنیک‌های پیچیده‌ای مانند «امضای حلقوی»[3]، «آدرس‌های مخفی»[4] و پروتکل‌های «اثبات بدون افشا»[5] استفاده می‌کنند تا اطلاعات مربوط به تراکنش‌ها، از جمله هویت فرستنده و گیرنده و میزان تراکنش‌ها، را به‌طور کامل مخفی نگه دارند. این قابلیت‌ها شناسایی و ردیابی تراکنش‌ها را برای نهادهای نظارتی و اجرای قانون به‌مراتب دشوارتر می‌کند [۱۴]. پرونده«Alpha Bay» ، که یکی از بزرگ‌ترین بازارهای غیرقانونی در دارک وب بود و در سال ۲۰۱۷ توسط نیروهای اجرای قانون تعطیل شد، نمونه‌ای بارز از استفاده گسترده از مونرو برای پولشویی است «Alpha Bay» .ابتدا از بیت‌کوین به‌عنوان ارز اصلی استفاده می‌کرد، اما با افزایش آگاهی از قابلیت‌های ردیابی بیت‌کوین، بسیاری از کاربران به رمزارز مونرو روی آوردند تا تراکنش‌های خود را به‌صورت کاملاً ناشناس انجام دهند. تحقیقات نشان داد که حجم قابل‌توجهی از تراکنش‌های مرتبط با مواد مخدر و سایر فعالیت‌های غیرقانونی در «Alpha Bay» از طریق مونرو انجام می‌شد. این امر تلاش‌های نهادهای اجرای قانون برای شناسایی و پیگیری مجرمان را به‌شدت پیچیده کرد[۱۵]. در ایران، عدم وجود زیرساخت‌های فنی کافی برای شناسایی و ردیابی این نوع رمزارزها، به پول‌شویان اجازه می‌دهد تا از رمزارزهایی مانند مونرو و زی‌کش برای پنهان‌سازی وجوه خود استفاده کنند. پرونده‌هایی نظیر «Alpha Bay» نشان داده‌اند که چگونه این نوع رمزارزها می‌توانند به‌طور مؤثر برای پولشویی مورد استفاده قرار گیرند. نهادهای نظارتی ایران باید از ابزارهای پیشرفته‌تری

---

[1] Anti-Money Laundering
[2] Know Your Customer
۳ - امضاهای حلقه (Ring Signatures) تکنیکی برای حفظ ناشناسی در تراکنش‌ها است که در رمزارزهایی مانند مونرو استفاده می‌شود. این روش به کاربران اجازه می‌دهد تا بدون فاش کردن هویت خود، تراکنش‌ها را امضا کنند، که این امر شناسایی منشأ وجوه غیرقانونی را دشوارتر کرده و چالش‌هایی برای نظارت و پیشگیری از پولشویی ایجاد می‌کند.

[4] Stealth Addresses
۵ - مدل‌های اثبات بدون افشا (Zero-Knowledge Proofs) تکنیکی است که به کاربران این امکان را می‌دهد که صحت اطلاعات را بدون فاش کردن جزئیات آن‌ها اثبات کنند. در زمینه رمزارزها، این روش می‌تواند برای پنهان‌سازی جزئیات تراکنش‌ها و محافظت از حریم خصوصی استفاده شود، اما همچنین می‌تواند مشکلاتی را برای نهادهای نظارتی در شناسایی و پیشگیری از پولشویی به همراه داشته باشد.

برای تحلیل و شناسایی این نوع تراکنش‌ها استفاده کنند و از همکاری‌های بین‌المللی برای مقابله با استفاده از رمزارزهای با حریم خصوصی بالا بهره‌برداری کنند.

۶- نقش یادگیری ماشینی در مبارزه با پولشویی

یادگیری ماشینی، مانند بسیاری از فناوری‌های نوین، می‌تواند به‌عنوان یک تیغ دولبه عمل کند؛ هم در تسهیل ارتکاب جرایم مالی نظیر پولشویی و هم در شناسایی و مبارزه با این جرایم. در ایران، با توجه به گسترش استفاده از رمزارزها و فقدان چارچوب‌های قانونی صریح در این زمینه، یادگیری ماشینی به‌عنوان ابزاری قدرتمند می‌تواند به نهادهای نظارتی کشور در شناسایی و پیشگیری از پولشویی کمک کند. اما در این مسیر، چالش‌هایی مانند نبود زیرساخت‌های فنی و آموزشی و همچنین نیاز به تدوین قوانین جدید باید برطرف شوند. در ادامه به برخی از مدل‌های پرکاربرد یادگیری ماشینی در این زمینه و نقش آن‌ها در شناسایی پولشویی پرداخته می‌شود:

۶-۱- رگرسیون لجستیک

رگرسیون لجستیک[1] یکی از مدل‌های پرکاربرد در یادگیری ماشینی است که برای پیش‌بینی احتمال وقوع رویدادهایی مانند پولشویی استفاده می‌شود. این مدل با تحلیل داده‌ها و ویژگی‌های تراکنش‌ها و رفتار کاربران، به شناسایی و پیش‌بینی پولشویی کمک می‌کند [۷]. در پرونده «بیتفینکس»[2] در سال ۲۰۱۶، که طی یک حمله هکری ۱۲۰،۰۰۰ رمزارز از نوع بیت‌کوین به سرقت رفت، از رگرسیون لجستیک برای شناسایی تراکنش‌های مشکوک استفاده شد [۱۶]. این مدل با تحلیل ویژگی‌هایی مانند حجم و فرکانس تراکنش‌ها و الگوهای رفتاری کاربران، توانست تراکنش‌های مشکوک مرتبط با پولشویی را شناسایی کند. در ایران، با وجود اصلاحات قانون مبارزه با پولشویی در سال ۱۳۹۷، نهادهای مالی و نظارتی همچنان نیازمند استفاده از مدل‌های یادگیری ماشینی نظیر رگرسیون لجستیک برای شناسایی و تحلیل تراکنش‌های مشکوک در سیستم‌های مالی کشور هستند.

۶-۲- درختان تصمیم

درختان تصمیم[3] در یادگیری ماشینی به‌عنوان یکی از ابزارهای قدرتمند برای طبقه‌بندی و تصمیم‌گیری شناخته می‌شوند. این مدل‌ها بر اساس ویژگی‌های داده‌ها، تصمیمات و پیش‌بینی‌هایی را به‌طور سیستماتیک و بصری انجام می‌دهند. درختان تصمیم به‌ویژه در شناسایی الگوهای پیچیده و قوانینی که ممکن است به پولشویی مربوط شوند، بسیار مؤثرند. در ایران، با توجه به اینکه رمزارزها به‌عنوان ابزاری برای پولشویی مورد استفاده قرار می‌گیرند، استفاده از درختان تصمیم در نهادهای نظارتی کشور می‌تواند به تحلیل دقیق‌تر داده‌های مالی و ردیابی تراکنش‌های مشکوک کمک کند. نهادهای نظارتی در ایران باید با بهره‌گیری از این مدل‌ها، توانایی خود را در شناسایی و پیشگیری از پولشویی تقویت کنند.

۶-۳- کاربرد درختان تصمیم در شناسایی پولشویی

درختان تصمیم با تقسیم داده‌ها به زیرمجموعه‌های کوچک‌تر و تحلیل ویژگی‌های مختلف مانند مقدار تراکنش‌ها، زمان و فرکانس، به شناسایی الگوهای غیرعادی و رفتارهای مشکوک کمک می‌کنند. در پرونده «کوین‌چک»[4]، یکی از بزرگ‌ترین صرافی‌های رمزارز ژاپن که در سال ۲۰۱۸ مورد حمله هکری قرار گرفت و ۵۰۰ میلیون دلار از رمزارز «نم» به سرقت رفت، از درختان تصمیم برای شناسایی الگوهای مشکوک استفاده شد. این مدل‌ها تراکنش‌هایی با مقادیر غیرمعمول بالا و از آدرس‌های ناشناخته را شناسایی کردند که به نهادهای نظارتی در بهبود توانایی شناسایی پولشویی کمک کرد. استفاده از درختان تصمیم در تحلیل داده‌های رمزارزها، نقش مهمی در تقویت امنیت و شفافیت دارد و به نهادهای نظارتی در اقدامات پیشگیرانه و واکنش سریع به فعالیت‌های مشکوک کمک می‌کند.

۶-۴- جنگل تصادفی

جنگل تصادفی تکنیکی پیشرفته در یادگیری ماشینی است که برای تحلیل داده‌های پیچیده و شناسایی الگوهای ناهنجار، از جمله در زمینه پیشگیری از پولشویی، کاربرد دارد. این مدل با استفاده از مجموعه‌ای از درختان تصمیم، توانایی پیش‌بینی و تحلیل را با ترکیب نتایج درختان تصادفی افزایش داده و خطر «اورفیتینگ» را کاهش می‌دهد. در حوزه پیشگیری از جرایم مالی نظیر پولشویی توسط رمزارزها، جنگل تصادفی به‌ویژه در شناسایی تراکنش‌های مشکوک بسیار مفید است. برای مثال، «بایننس»، یکی از بزرگ‌ترین صرافی‌های رمزارز، در سال ۲۰۱۸ از جنگل تصادفی برای تحلیل تراکنش‌های کاربران استفاده کرد. این تکنیک به شناسایی الگوهای غیرعادی و مشکوک، مانند تراکنش‌های مکرر و حجم بالای مبالغ که ممکن است به پولشویی توسط رمزارزها مرتبط باشند، کمک کرد [۱۱]. در ایران، با توجه به رشد تراکنش‌های رمزارزی و چالش‌های ناشی از نبود زیرساخت‌های نظارتی قوی، استفاده از جنگل تصادفی می‌تواند به شناسایی تراکنش‌های مشکوک در صرافی‌ها و دیگر نهادهای مالی کمک کند. این تکنیک به نهادهای مالی ایران امکان می‌دهد تا تراکنش‌های غیرعادی را به‌طور دقیق‌تر شناسایی کنند و از پیشرفت فعالیت‌های پولشویی جلوگیری کنند. در مقام تبیین مزایای استفاده از جنگل تصادفی باید گفت این شیوه

---

[1] Categorical Data

۲ - صرافی Bitfinex کی از بزرگ‌ترین و شناخته‌شده‌ترین صرافی‌های رمزارز در جهان است که در سال ۲۰۱۲ تأسیس شد و به‌طور ویژه به دلیل حجم بالای معاملات و امکانات پیشرفته‌اش برای معامله‌گران حرفه‌ای شهرت دارد. این صرافی در مدت زمان فعالیت خود با برخی چالش‌ها و مسائل امنیتی مواجه شده است که توجهات زیادی را جلب کرده است.

[3] Decision Trees

[4] Coin check

شـــامل دقت بـالا، پیشـــگیری از «اورفیتینـگ»[1] و توانـایی تحلیـل ناهنجاری‌ها اســت. با توجه به این ویژگی‌ها، جنگل تصـــادفی به‌عنوان یک ابزار مؤثر در شـــناســـایی پولشـــویی و تحلیل داده‌های پیچیده در زمینه رمزارزها شناخته می‌شود. این تکنیک با قابلیت‌های خود، به‌طور مؤثری در نظارت و مبارزه با پولشـــویی در صـــرافی‌های رمزارز و دیگر نهادهای مالی دیجیتال به کار گرفته می‌شـود و به شـناسـایی الگوهای غیرعادی و پیش‌بینی فعالیت‌های مشکوک کمک می‌کند.

۶-۵- ماشین‌های بردار پشتیبان

ماشـــین‌های بردار پشـــتیبان[2] ابزارهای مؤثری در یادگیری ماشـــینی هســـتند که برای طبقه‌بندی داده‌ها و تحلیل الگوهای پیچیده به کار می‌روند. این مـدل‌هـا بـا ایجـاد مرزهـای تصـــمیم‌گیری برای تفکیـک کلاس‌ها، قادر به شناسایی ناهنجاری‌ها و الگوهای پیچیده در داده‌ها، از جمله تراکنش‌های مشـکوک و پولشـویی هسـتند. در پرونده مرتبط با صـــرافی رمزارز «BTC-e»، این ماشـــین‌ها به‌عنوان ابزار کلیدی برای شناسایی و تحلیل تراکنش‌های غیرقانونی استفاده شدند. در سال‌های ۲۰۱۷ و ۲۰۱۸، صـــرافی «BTC-e» به دلیل ارتباط با فعالیت‌های پولشـــویی تحت تحقیق قرار گرفت و تحلیلگران بـا بهره‌گیری از ماشـــین‌های بردار پشـــتیبان توانســـتند تراکنش‌های غیرعادی، از جمله تراکنش‌هـای بزرگ و مکرر کـه ممکن بود نشـــانـه‌هـایی از عملیـات پولشـویی باشـند، شـناسـایی کنند [۱۷]. مزایای این تکنیک شامل دقت بالا، توانایی تحلیل داده‌های با ابعاد بالا و شـــناســـایی الگوهای پیچیده اسـت. این ویژگی‌ها ماشـین‌های بردار پشـتیبان را به ابزاری ارزشـمند برای نهادهای نظارتی تبدیل کرده اســـت، به‌ویژه در پیشـــگیری از پولشـــویی و تحلیل فعالیت‌های مالی غیرقانونی در فضـــای رمزارزها. در ایران، نهادهای نظارتی می‌توانند از ماشـــین‌های بردار پشـــتیبان برای شـــنـاســـایی تراکنش‌های غیرعادی اســـتفاده کنند و از آن در تحلیل تراکنش‌های مشـــکوک در فضـــای رمزارزها بهره ببرند. با توجه به پیچیدگی‌های موجود در فضـای مالی ایران و اسـتفاده‌های غیرقانونی از رمزارزها، این مدل می‌تواند به پیشگیری از پولشویی کمک کند.

۶-۶- شبکه‌های پیچشی گراف

شبکه‌های پیچشی گراف[3] مدل‌های پیشرفته در یادگیری ماشینی هستند که به‌ویژه برای تحلیل داده‌های گراف و شبکه‌های پیچیده، نظیر تراکنش‌های رمزارز و روابط بین کاربران، کاربرد دارند. این مدل‌ها با استفاده از تکنیک‌های پیچشی برای داده‌های گراف، قادرند الگوهای مخفی و ساختارهای پیچیده را شبیه‌سازی و تحلیل کنند. به‌عبارت دیگر، این شبکه‌های پیچشی گراف برای پردازش داده‌های ساختاریافته به شکل گراف طراحی شده‌اند و می‌توانند روابط بین نودها (کاربران، تراکنش‌ها و غیره) را به‌طور دقیق بررسی کنند. یکی از ویژگی‌های مهم این شبکه‌ها توانایی در شناسایی الگوهای پیچیده و روابط پنهان است که به شناسایی فعالیت‌های غیرعادی و پولشویی کمک می‌کند. در ایران، استفاده از شبکه‌های پیچشی گراف می‌تواند به نهادهای نظارتی کمک کند تا الگوهای مخفی و روابط پیچیده بین تراکنش‌های رمزارزی و کاربران را شناسایی کنند. این مدل‌ها به نهادهای امنیتی ایران امکان می‌دهند که فعالیت‌های غیرعادی و پولشویی را با دقت بیشتری شناسایی و پیگیری کنند.

۷- تحلیل مزایا و معایب استفاده از یادگیری ماشینی در مهار پولشویی با رمزارزها

۷-۱- مزایا

در تحلیل پولشویی از طریق رمزارزها، استفاده از یادگیری ماشینی، به‌ویژه به‌دلیل مزایای متعدد آن در دقت و کارایی، توانایی یادگیری از داده‌های جدید و کاهش نیاز به نظارت سنتی و دستی، به ابزاری قدرتمند در این زمینه تبدیل شده است. این تکنیک‌ها می‌توانند در شناسایی فعالیت‌های غیرقانونی پیچیده و الگوهای مخفی، به‌ویژه در زمینه وقوع جرم پولشویی توسط رمزارزها که دارای حجم بالای داده‌ها و پیچیدگی‌های ساختاری هستند، به‌طور مؤثری عمل کنند. یکی از مزایای بارز یادگیری ماشینی، دقت و کارایی بالای آن در تحلیل داده‌های پیچیده است. مدل‌های پیشرفته‌ای مانند شبکه‌های عصبی و شبکه‌های پیچشی گراف به‌طور ویژه برای شناسایی الگوهای پیچیده و ناهنجاری‌های پنهان طراحی شده‌اند. این مدل‌ها به تحلیل دقیق‌تر روابط پیچیده بین ویژگی‌های تراکنش‌ها و شبیه‌سازی فعالیت‌های غیرقانونی نظیر پولشویی کمک کردند. توانایی یادگیری از داده‌های جدید، مزیت دیگر یادگیری ماشینی است. مدل‌های یادگیری ماشینی می‌توانند با دریافت داده‌های تازه و به‌روز، به‌طور مداوم بهبود یابند و نتایج دقیق‌تری ارائه دهند. این ویژگی، به‌ویژه در دنیای رمزارزها که الگوهای فعالیت ممکن است به‌سرعت تغییر کنند، بسیار ارزشمند است. برای مثال، در مورد تحلیل تراکنش‌های مرتبط با صرافی‌های بزرگ مانند «Binance»، مدل‌های یادگیری ماشینی قادر بودند با پردازش داده‌های جدید و تحلیل الگوهای به‌روز، به شناسایی فعالیت‌های مشکوک و پولشویی کمک کنند. علاوه بر این، استفاده از یادگیری ماشینی می‌تواند نیاز به نظارت دستی و تحلیل‌های انسانی را کاهش دهد. در پردازش داده‌های بزرگ و پیچیده، این تکنیک‌ها به‌طور خودکار قادر به شناسایی ناهنجاری‌ها و فعالیت‌های غیرقانونی هستند، به‌ویژه در مواقعی که حجم داده‌ها بسیار زیاد است، می‌تواند مفید واقع شود. این قابلیت باعث می‌شود که تحلیلگران بتوانند بر روی بررسی‌های استراتژیک و

---

[1] خطر اورفیتینگ (Overfitting) زمانی رخ می‌دهد که یک مدل یادگیری ماشینی به حدی به داده‌های آموزشی خود تطابق پیدا می‌کند که قادر به تعمیم خوب به داده‌های جدید نباشد. به عبارت دیگر، مدل به جزئیات و نویزهای خاص داده‌های آموزشی به شدت وابسته می‌شود و از الگوهای عمومی و واقعی که در داده‌های جدید نیز وجود دارد، غفلت می‌کند.

[2] Support vector machines

[3] Convolutional Neural Network

تصمیم‌گیری‌های کلیدی تمرکز کنند، در حالی که مدل‌های یادگیری ماشینی به‌طور خودکار داده‌ها را تحلیل و گزارش‌های مورد نیاز را تولید می‌کنند [۱۲]. به‌طور کلی، استفاده از یادگیری ماشینی در شناسایی پولشویی از طریق رمزارزها، با بهره‌گیری از دقت بالا، توانایی یادگیری از داده‌های جدید و کاهش نیاز به نظارت دستی، توانسته است به‌طور قابل توجهی در بهبود فرآیندهای تحلیل و شناسایی فعالیت‌های غیرقانونی کمک کند. این تکنیک‌ها، اگرچه به همراه چالش‌هایی هستند، اما همچنان به‌عنوان ابزارهای مؤثری در مبارزه با پولشویی و فعالیت‌های غیرقانونی در دنیای دیجیتال شناخته می‌شوند.

۷-۲- معایب و چالش‌های فنی-حقوقی

توسعه و پیاده‌سازی مدل‌های یادگیری ماشینی برای شناسایی پولشویی از طریق رمزارزها، علی‌رغم مزایای زیادی که دارد، با چالش‌های قابل‌توجهی نیز همراه است. این چالش‌ها شامل پیچیدگی و هزینه، احتمال اورفیتینگ و مسائل مربوط به تفسیرپذیری می‌شود که در ادامه به تفصیل مورد بررسی قرار می‌گیرد. یکی از مشکلات اصلی در استفاده از مدل‌های یادگیری ماشینی در زمینه شناسایی عملیات جرم پولشویی، پیچیدگی و هزینه‌های بالای آن است. توسعه و پیاده‌سازی این مدل‌ها نیازمند منابع محاسباتی گسترده و تخصص در زمینه‌های مربوط به یادگیری ماشینی و تحلیل داده‌ها است. دیگر چالش مهم در این زمینه، احتمال اورفیتینگ مدل‌های موجود در یادگیری ماشینی است. اورفیتینگ به وضعیتی اشاره دارد که در آن مدل یادگیری ماشینی به‌طور بیش از حد به داده‌های آموزشی تطبیق می‌یابد و در نتیجه عملکرد آن در مواجهه با داده‌های جدید کاهش می‌یابد [۹]. در ایران، هزینه‌های بالای پیاده‌سازی این فناوری یکی از موانع اصلی است. در زمینه شناسایی جرم پولشویی، این موضوع می‌تواند به‌ویژه مشکل‌ساز باشد. به‌عنوان مثال، در استفاده از شبکه‌های عصبی عمیق برای تحلیل الگوهای پولشویی، این مدل‌ها ممکن است به‌طور خاص با داده‌های آموزشی خود تطبیق یابند و نتایج نادرستی در داده‌های واقعی ارائه دهند. این موضوع می‌تواند بر دقت و قابلیت اعتماد مدل‌ها تأثیر بگذارد و نیازمند استراتژی‌های مناسب برای تنظیم و ارزیابی مدل‌ها باشد.

علاوه بر این، مسائل مربوط به تفسیرپذیری نیز یکی از چالش‌های بزرگ در استفاده از مدل‌های یادگیری ماشینی است. بسیاری از مدل‌های پیچیده مانند شبکه‌های عصبی عمیق، به‌دلیل ساختار پیچیده و تعداد بالای پارامترها، به‌سختی قابل تفسیر هستند. این مسئله می‌تواند در تحلیل و توضیح نتایج به نهادهای نظارتی مشکل‌ساز باشد. برای مثال، در پرونده مربوط به استفاده از مدل‌های یادگیری ماشینی برای شناسایی پولشویی در صرافی«Bitfinex» ، تحلیلگران با مشکل توضیح و تفسیر دقیق نتایج مدل‌های پیچیده مواجه شدند. این مسئله، به‌ویژه زمانی که نتایج مدل باید به مقامات نظارتی ارائه شود و نیاز به توضیحات شفاف و قابل‌فهم دارد، می‌تواند چالش‌برانگیز باشد [۹]. در نتیجه، استفاده از یادگیری ماشینی در شناسایی پولشویی از طریق رمزارزها، با وجود مزایای چشمگیر آن، نیازمند توجه به چالش‌های مرتبط با پیچیدگی و هزینه‌های توسعه، احتمال اورفیتینگ و مسائل تفسیرپذیری است. این چالش‌ها باید به‌دقت مدیریت شوند تا بتوان از این تکنیک‌های پیشرفته به‌طور مؤثر در مبارزه با پولشویی و فعالیت‌های غیرقانونی در حوزه رمزارزها بهره‌برداری کرد. پیاده‌سازی الگوریتم‌های یادگیری ماشینی در حوزه مبارزه با پولشویی، با وجود پتانسیل‌های بالا، با چالش‌های فنی و اجرایی متعددی روبه‌روست:

۱. پیاده‌سازی الگوریتم‌های یادگیری ماشینی به‌عنوان یکی از ابزارهای نوین در مقابله با پولشویی در تراکنش‌های رمزارزی، با چالش‌های فنی و اجرایی مختلفی مواجه است. یکی از مهم‌ترین این چالش‌ها، نیاز به داده‌های با حجم و کیفیت بالاست. کیفیت داده‌ها به‌طور مستقیم بر دقت مدل‌های یادگیری ماشینی تأثیر می‌گذارد. داده‌های ناقص یا نادرست می‌توانند منجر به نتایج غیرقابل‌اعتماد شوند، چنان‌که در پرونده صرافی «BTC-e» مشاهده شد [۱۸]. در ایران، یکی از بزرگ‌ترین چالش‌ها، کیفیت داده‌ها است. برای پیاده‌سازی یادگیری ماشینی به داده‌های با کیفیت و جامع نیاز است، اما داده‌های موجود در نهادهای مالی و نظارتی کشور ممکن است ناقص یا نادرست باشند. برای مثال، در پرونده‌های مرتبط با صرافی‌های رمزارز در کشور، نقص در داده‌های مربوط به تراکنش‌ها می‌تواند به شناسایی نادرست فعالیت‌های مشکوک منجر شود و باعث سردرگمی نهادهای نظارتی گردد. این امر بر ضرورت ارتقای کیفیت داده‌ها و زیرساخت‌های داده‌ای در کشورهایی چون ایران تأکید دارد. از سوی دیگر، یکی از چالش‌های عمده در حوزه استفاده از یادگیری ماشینی برای شناسایی پولشویی، نیاز به انطباق مداوم مدل‌ها با تغییرات مستمر در روش‌های پولشویی است. پول‌شویان همواره تکنیک‌های جدید و پیچیده‌تری را به‌کار می‌گیرند تا از سیستم‌های نظارتی عبور کنند [۱۲].

۲. علاوه بر این، الگوریتم‌های یادگیری ماشینی، به‌ویژه مدل‌های یادگیری عمیق، نیازمند منابع محاسباتی گسترده‌ای هستند. این مدل‌ها با ساختار پیچیده و تعداد زیاد پارامترهای قابل آموزش، به پردازنده‌های پیشرفته، حافظه زیاد و واحدهای پردازش گرافیکی[1] برای تحلیل حجم زیادی از داده‌ها نیاز دارند. اجرای این مدل‌ها، به‌ویژه در سازمان‌های کوچک با منابع محدود، چالش‌برانگیز است و می‌تواند هزینه‌های عملیاتی را افزایش دهد. بنابراین، سازمان‌ها باید در ارتقای توانایی‌های محاسباتی خود سرمایه‌گذاری کنند و زیرساخت‌های مناسبی را برای بهره‌برداری مؤثر از این تکنیک‌ها فراهم آورند.

در مجموع، استفاده از الگوریتم‌های یادگیری ماشینی در شناسایی و پیشگیری از پولشویی در تراکنش‌های رمزارزی به‌عنوان یک ابزار پیشرفته و ضروری، با چالش‌های فنی و اجرایی مختلفی همراه است. ارتقای کیفیت داده‌ها، به‌روزرسانی مداوم الگوریتم‌ها و تأمین منابع محاسباتی کافی از جمله الزامات اصلی در این زمینه هستند. با این حال، با رفع این چالش‌ها و ایجاد زیرساخت‌های مناسب، می‌توان به بهره‌برداری مؤثر از این تکنیک‌ها امیدوار بود و گامی مؤثر در جهت

[1] Graphical Processing Units

پیشگیری از پولشویی و تقویت سیاست جنایی در قبال رمزارزها برداشت. پیاده‌سازی الگوریتم‌های یادگیری ماشینی در مبارزه با پولشویی همچنین با مشکلات قانونی و مقرراتی خاصی روبه‌روست:

پیاده‌سازی الگوریتم‌های یادگیری ماشینی در مبارزه با پولشویی در تراکنش‌های رمزارزی، علاوه بر مزایای متعدد، با چالش‌های قانونی و مقرراتی قابل‌توجهی روبه‌رو است. یکی از مهم‌ترین این چالش‌ها، عدم تنظیم‌گری و استانداردسازی مناسب در این زمینه است [۱۹]. لذا چالش‌های قانونی و مقرراتی یکی از مشکلات اصلی در استفاده از یادگیری ماشینی در ایران است. در حال حاضر، قوانین و مقررات خاصی برای نظارت و استفاده از این فناوری در زمینه شناسایی پولشویی در کشور وجود ندارد. نبود استانداردهای مشخص می‌تواند به مشکلاتی در اجرای مدل‌های یادگیری ماشینی منجر شود. برای مثال، حادثه حمله هکری گسترده به صرافی «Bitfinex» در سال ۲۰۱۶ نشان داد که نبود چارچوب‌های قانونی و نظارتی و عدم استانداردها و مقررات کافی می‌تواند به مشکلات جدی در امنیت و کارایی سیستم‌ها منجر شود. هکرها با بهره‌برداری از ضعف‌های امنیتی و نبود استانداردهای مشخص، مقدار زیادی رمزارز را از حساب‌های کاربران سرقت کردند که مشخص می‌تواند باعث آسیب‌پذیری سیستم‌های مالی شود. در ایران، تدوین و اجرای استانداردهای قانونی و نظارتی دقیق برای استفاده از یادگیری ماشینی در شناسایی پولشویی، یک نیاز اساسی است که باید مورد توجه سیاست‌گذاران قرار گیرد. این حادثه نشان‌دهنده ضرورت تدوین چارچوب‌های قانونی و مقرراتی خاص ذیل سیاست جامع هوشمند برای استفاده از یادگیری ماشینی در شناسایی جرم پولشویی در حوزه رمزارزها است. یکی دیگر از چالش‌ها، مسائل حقوقی و اعتبار مدل‌های یادگیری ماشینی در دادگاه‌ها و نزد نهادهای قضایی است. در ایران، نهادهای نظارتی ممکن است با مشکلاتی در پذیرش نتایج حاصل از این مدل‌ها مواجه شوند، به‌ویژه در مواردی که تصمیمات مبتنی بر این مدل‌ها به مسدودسازی حساب‌های کاربران یا اعمال جریمه‌های قانونی منجر می‌شود. برای مثال، در پرونده «Crypto Capital»[1] در سال ۲۰۱۹، استفاده از این الگوریتم‌ها باعث شناسایی نادرست برخی تراکنش‌های مشروع به‌عنوان فعالیت‌های مشکوک شد. این اشتباهات منجر به مسدود شدن حساب‌های کاربران و بروز مشکلات حقوقی قابل توجهی برای شرکت شد. کاربران به دلیل مسدود شدن غیرقانونی حساب‌هایشان دعاوی حقوقی علیه شرکت مطرح کردند که این مسئله منجر به بروز مشکلات حقوقی برای شرکت و کاهش اعتماد عمومی شد [۱۱]. این موضوع نشان می‌دهد که توسعه و استفاده از الگوریتم‌های یادگیری ماشینی باید با دقت، نظارت بسیار بالا همراه با به‌روزرسانی‌های مستمر باشد و در عین حال سازوکارهای جبران خسارت به‌طور جدی مورد توجه قرار گیرد تا حقوق قانونی کاربران رعایت و از مشکلات مشابه جلوگیری گردد. در نهایت، یکی دیگر از چالش‌های مهم، شفافیت و پاسخگویی الگوریتم‌ها است. مدل‌های پیچیده یادگیری ماشینی، مانند شبکه‌های عصبی عمیق، ممکن است به‌سختی قابل تفسیر باشند. به‌عنوان مثال، در پرونده «Bitfinex» در سال ۲۰۱۹، این صرافی به دلیل استفاده از الگوریتم‌های پیچیده برای شناسایی عملیات پولشویی، قادر به ارائه توضیحات واضحی درباره تصمیمات خود نبود که این مسئله منجر به فشار نهادهای نظارتی، مشکلات قانونی و کاهش اعتماد به سیستم‌های تحلیل داده‌های صرافی شد [۱۹]. این امر می‌تواند در ایران، به‌ویژه زمانی که نهادهای نظارتی نیاز به توضیحات شفاف درباره تصمیمات الگوریتمی دارند، مشکل‌ساز شود. برای رفع این چالش، نیاز است که نهادهای نظارتی کشور از تکنیک‌های تفسیرپذیری در مدل‌های خود استفاده کنند تا بتوانند پاسخگوی تصمیمات مبتنی بر یادگیری ماشینی باشند. در مجموع، استفاده از الگوریتم‌های یادگیری ماشینی در شناسایی و پیشگیری از پولشویی در تراکنش‌های رمزارزی نیازمند تنظیم و استانداردسازی دقیق، توجه به مسائل قضایی و حقوقی، و بهبود شفافیت و پاسخگویی الگوریتم‌ها است. تنها با رعایت این موارد می‌توان از کارایی و امنیت این الگوریتم‌ها بهره‌مند شد و از بروز تبعات و مشکلات قانونی جلوگیری کرد.

۸- جایگاه حقوقی یادگیری ماشینی در سیاست جنایی مهار پولشویی با تراکنش‌های رمزارزی

استفاده از یادگیری ماشینی در شناسایی پولشویی در تراکنش‌های رمزارزی موضوعی است که در سطح بین‌المللی و منطقه‌ای توجه بسیاری را به خود جلب کرده است. این فناوری، به‌ویژه در زمینه سیاست‌های جنایی و مسائل حقوقی، نشان‌دهنده نیاز به بررسی و تطبیق قوانین و مقررات موجود با فناوری‌های نوین در این زمینه است. در سطح بین‌المللی، گروه ویژه اقدام مالی (FATF) به‌طور مستقیم به استفاده از یادگیری ماشینی اشاره نکرده است، اما تأکید می‌کند که کشورها باید از فناوری‌های پیشرفته برای ارتقای کارایی سیستم‌های نظارتی خود بهره ببرند. این نهاد به کشورهای عضو توصیه می‌کند که از تکنولوژی‌های نوین برای مقابله با پولشویی و تأمین مالی تروریسم استفاده کنند. در اتحادیه اروپا، «دستورالعمل‌های مبارزه با پولشویی» نیز بر اهمیت استفاده از ابزارهای فناورانه دیجیتال و تحلیل داده‌ها تأکید دارد، هرچند به‌طور خاص به یادگیری ماشینی اشاره نکرده است. در ایالات متحده، قوانین و نهادهای نظارتی مانند «شبکه اجرای جرایم مالی» از استفاده از فناوری‌های نوین برای شناسایی و گزارش تراکنش‌های مشکوک حمایت می‌کنند، هرچند یادگیری ماشینی به‌طور مستقیم در قوانین ذکر نشده است. سازمان‌های بین‌المللی مانند بلنک جهانی و صندوق بین‌المللی پول [2] نیز بر اهمیت این فناوری‌ها

[1] Crypto Capital، در سال ۲۰۱۳ تأسیس شده و به‌عنوان یک شرکت خدمات مالی و پردازش پرداخت‌های رمزارزی فعالیت می‌کرد. این شرکت به‌طور گسترده به صرافی‌های رمزارز و کسب‌وکارهای آنلاین خدمات می‌داد و در سال ۲۰۱۹ به دلیل ارتباط با پولشویی و مشکلات قانونی تحت بررسی شدید قرار گرفت. در پی این مشکلات، شرکت مزبور به دلیل نقض قوانین ضدپولشویی و ارتباط با فعالیت‌های غیرقانونی، تحت فشارهای قانونی و مسدود شدن حساب‌های بانکی قرار گرفت.

[2] International Monetary Fund

تأکید دارند و از کشورهای عضو خواسته‌اند که از یادگیری ماشینی برای بهبود سیستم‌های نظارتی خود استفاده کنند.

در ایران، قانون مبارزه با پولشویی مصوب ۱۳۸۶ و آیین‌نامه اجرایی آن، چارچوب قانونی اصلی برای مقابله با پولشویی را تشکیل می‌دهند. هرچند این قانون بر استفاده از فناوری‌های نوین تأکید کرده است، ولی به‌طور مستقیم به یادگیری ماشینی اشاره نمی‌کند. اصلاحات جدیدی که در سال ۱۳۹۷ در این قانون اعمال شده است، بر اهمیت ارتقای کارایی سیستم‌های نظارتی با استفاده از فناوری‌های پیشرفته تأکید دارند، اما همچنان جای کار دارد تا استفاده خاص از یادگیری ماشینی به‌طور مستقیم در قوانین گنجانده شود. در ایران، چالش‌هایی در زمینه به‌کارگیری یادگیری ماشینی برای مقابله با جرم پولشویی توسط رمزارزها وجود دارد. عدم وجود چارچوب‌های قانونی صریح، نیاز به توسعه زیرساخت‌های فنی و آموزشی، و محدودیت‌های بین‌المللی از جمله مشکلاتی هستند که باید برطرف شوند. برای استفاده مؤثر از یادگیری ماشینی، نهادهای مالی و نظارتی نیاز به تدوین مقررات جدید و به‌روزرسانی قوانین دارند؛ همچنین باید به آموزش‌های لازم برای پرسنل و فراهم کردن زیرساخت‌های فنی مناسب توجه کنند.

پولشویی در تراکنش‌های رمزارزی، به دلیل ویژگی‌هایی مانند ناشناس بودن و جهانی بودن این تراکنش‌ها، یک چالش بزرگ برای نهادهای نظارتی و اجرای قانون است. استفاده از یادگیری ماشینی در شناسایی و پیشگیری از جرائم این حوزه، به‌ویژه پولشویی، به‌عنوان یک ابزار کلیدی و اثرگذار در اجرای سیاست جنایی مقتضی در این حوزه شناخته می‌شود. این فناوری می‌تواند نقش مهمی در ساختار سیاست جنایی پیشگیرانه، فناورانه، اقتصادی، اجرایی و مشارکتی ایفا کند و تولنایی آن در تحلیل داده‌های مالی پیچیده، به نهادهای نظارتی امکان می‌دهد تا با دقت بیشتری به مقابله با پولشویی در فضای رمزارزی بپردازند. «سایت‌های جعلی با استفاده از تبلیغات گسترده در فضای مجازی سعی در کسب اعتماد مردم می‌کنند تا آنها با پرداخت مبالغی، برای آنها حساب کاربری و کیف پول دیجیتالی ایجاد کنند. آگاه‌سازی کاربران از گذر برگزاری کلاس‌های آشنایی با رمزارزها و همچنین فیلترینگ سایت‌های مشکوک به ارتکاب فعل مجرمانه» [۲۰]. در قالب سطوح سیاست جنایی پیشگیرانه وضعی و اجتماعی، تقنینی و قضائی و اجرائی و مشارکتی ضروری است.

سیاست جنایی پیشگیرانه به دنبال ممانعت از وقوع جرم قبل از ارتکاب آن است. این سیاست بر شناسایی و کاهش عوامل و فرصت‌های جرم‌زایی متمرکز است تا به‌طور مؤثری از وقوع جرم جلوگیری کند. در زمینه پولشویی در زمینه رمزارزها، یادگیری ماشینی به‌عنوان یک ابزار پیشگیرانه برجسته عمل می‌کند. با استفاده از الگوریتم‌های یادگیری ماشینی، می‌توان رفتارهای مالی غیرعادی را شناسایی کرده و به‌طور زودهنگام به مقامات مربوطه اطلاع داد تا از پیشرفت فعالیت‌های پولشویی جلوگیری شود. سیاست جنایی فنی و فناورانه بر کاربرد فناوری‌های پیشرفته برای مقابله با جرائم پیچیده و نوظهور تأکید دارد. در مورد پولشویی دیجیتال، یادگیری ماشینی به‌عنوان یک ابزار فنی پیشرفته، نقشی کلیدی ایفا می‌کند. فناوری‌هایی مانند «جنگل‌های تصادفی» و «شبکه‌های عصبی عمیق» به تحلیل دقیق‌تر و شناسایی مؤثرتر تراکنش‌های مشکوک کمک می‌کنند. به‌طور مثال، در ایالات متحده، در سال ۲۰۱۹، شرکت‌های فناوری با استفاده از الگوریتم‌های یادگیری ماشینی موفق به شناسایی یک شبکه پولشویی بین‌المللی شدند که از تراکنش‌های رمزارزی برای پنهان کردن فعالیت‌های غیرقانونی خود استفاده می‌کردند. این نوع فناوری‌های پیشرفته به مقامات و نهادهای مالی این امکان را می‌دهند که با دقت بیشتری به تحلیل داده‌ها بپردازند و فعالیت‌های پولشویی را شناسایی کنند؛ که این امر بهبود قابل توجهی در فرآیندهای نظارتی و اجرائی به همراه دارد [۱۲].

سیاست جنایی اجرائی بر اجرای قوانین و مقررات مربوط به مبارزه با جرائم توسط نهادهای اجرائی مانند پلیس، دادستانی و دستگاه قضائی تمرکز دارد. یادگیری ماشینی می‌تواند کارایی و دقت این نهادها را در شناسایی و مقابله با پولشویی افزایش دهد. این موضوع نشان‌دهنده توانایی یادگیری ماشینی در ارتقاء فرآیندهای اجرائی و قضائی و تقویت اقدامات قانونی در مقابله با جرم پولشویی توسط رمزارزها است. به‌طور مثال، در سال ۲۰۲۱، دادستانی فدرال ایالات متحده از تحلیل‌های مبتنی بر یادگیری ماشینی برای شناسایی و تعقیب یک شبکه گسترده پولشویی که از طریق رمزارزها فعالیت می‌کرد، استفاده کرد. این تحلیل‌ها به‌عنوان شواهد دیجیتال در پرونده‌های قضائی مورد استفاده قرار گرفت و منجر به محکومیت عاملان شد [۲۱]. سیاست جنایی مشارکتی بر همکاری و هماهنگی بین نهادهای دولتی و خصوصی و نهادهای بین‌المللی برای مقابله با جرائم تأکید دارد. استفاده از یادگیری ماشینی در شناسایی پولشویی نیازمند همکاری نزدیک بین این نهادها است. به‌عنوان مثال، گروه FATFبا همکاری بانک‌های بین‌المللی و شرکت‌های فناوری، سیستم یادگیری ماشینی را برای شناسایی تراکنش‌های مشکوک در سطح جهانی توسعه داد. این همکاری منجر به شناسایی و مسدودسازی میلیون‌ها دلار پولشویی از طریق تراکنش‌های رمزارزی شد. این نمونه تأکید می‌کند که سیاست جنایی مشارکتی با استفاده از فناوری‌های نوین و همکاری‌های بین‌المللی می‌تواند به شناسایی و مقابله مؤثرتر با پولشویی کمک کند [۹]. همکاری‌های بین‌المللی و تبادل اطلاعات در این زمینه به بهبود کارایی و دقت الگوریتم‌های یادگیری ماشینی در شناسایی فعالیت‌های غیرقانونی کمک شایانی می‌کند.

۹- نتیجه‌گیری

این پژوهش به بررسی نقش یادگیری ماشینی در شناسایی و پیشگیری از پولشویی در تراکنش‌های رمزارزی پرداخته است. الگوریتم‌های پیشرفته‌ای مانند جنگل تصادفی، XGBoost، شبکه‌های پیچشی گراف و شبکه‌های عصبی عمیق در شناسایی الگوهای مشکوک و پنهان که ممکن است از دید روش‌های نظارتی سنتی پنهان بمانند، بسیار مؤثر عمل می‌کنند. این مدل‌ها با تحلیل داده‌های عظیم و پیچیده، امکان شناسایی دقیق‌تر و سریع‌تر فعالیت‌های پولشویی را فراهم

می‌آورند. همچنین، یادگیری ماشـــینی به‌عنوان بخشـــی از رویکردهای سـیاسـت جنایی پیشـگیرانه در حوزه رمزارزها، نقشـی کلیدی در بهبود کارایی نهادهای نظارتی ایفا می‌کند.

نتایج این تحقیق نشان داد که یادگیری ماشینی می‌تواند به شکل مؤثری به شـناسـایی و پیشـگیری از پولشـویی در تراکنش‌های رمزارزی کمک کند. یافته‌های مقاله نشان می‌دهد که:

- پاســخ بـه پرســش اول: یـادگیری مـاشـــینی می‌توانـد چارچوب‌های نظارتی و حقوقی برای مقابله با پولشـویی را بهبود بخشـد. با بهره‌گیری از این تکنیک‌ها، نهادهای نظارتی قادر خواهند بود تا الگوهای مشکوک در تراکنش‌های رمزارزی را شناسایی کرده و از وقوع جرم‌های مالی جلوگیری کنند.
- پاسخ به پرسش دوم: الگوریتم‌های یادگیری ماشینی مانند شبکه‌های عصبی عمیق و مدل‌های پیچشی گراف می‌توانند به شناسایی الگوهای غیرعادی و پیچیده در تراکنش‌های رمزارزی کمک کنند. این فناوری‌ها امکان تحلیل حجم بالای داده‌ها را فراهم می‌کنند و می‌توانند به‌طور مداوم با داده‌های جدید به‌روزرسـانی شـوند تا در برابر روش‌های جدید پولشویی عملکرد بهتری داشته باشند.
- پاسخ به پرسش سوم: در زمینه تدوین سیاست‌های جنایی هوشـــمندانه، یادگیری ماشـــینی به نهادهای نظارتی کمک می‌کند تا سـیاسـت‌های پیشـگیرانه و مبتنی بر داده‌ها را اتخاذ کنند که به کاهش جرایم مالی نظیر پولشویی کمک می‌کند. همچنین استفاده از یادگیری ماشـــینی نیازمند تقویت همکاری‌های بین‌المللی اســـت تا قوانین و چارچوب‌های نظارتی جهانی بتوانند بهتر با چالش‌های رمزارزی مقابله کنند.

در پایان، با توجه به اهمیت اســـتفاده از یادگیری ماشـــینی در شـناسـایی و پیشـگیری از پولشـویی در ایران، پیشـنهادات کاربردی زیر ارائه می‌شود:

۱- تدوین چارچوب‌های قانونی و مقرراتی: ســـیاســـت‌گذاران ایران باید مقررات و چارچوب‌های قانونی مناسـب برای اسـتفاده از یادگیری ماشینی در شـناسـایی و مبارزه با پولشـویی را تدوین کنند. این مقررات باید جمع‌آوری و پردازش داده‌ها را تسـهیل کرده و در عین حال حریم خصـوصـی کاربران را حفظ کنند. همکاری با نهادهای بین‌المللی برای هماهنگی بیشتر در این زمینه نیز ضروری است.

۲- تقویت زیرساخت‌های نظارتی و آموزشی: نهادهای نظارتی ایران باید در جهت توسـعه زیرسـاخت‌های نظارتی برای به‌کارگیری یادگیری ماشینی در تحلیل تراکنش‌های رمزارزی سرمایه‌گذاری کنند. همچنین، آموزش نیروی انسانی و تقویت مهارت‌های نظارتی برای استفاده مؤثر از این فناوری از اهمیت بالایی برخوردار است.

۳- بهبود کیفیت داده‌ها و توســـعه مدل‌های یادگیری ماشـــینی: داده‌های تراکنش‌های رمزارزی باید به‌طور مستمر به‌روزرسانی و کیفیت داده‌ها بهبود یابد تا مدل‌های یادگیری ماشـــینی با داده‌های دقیق و صـــحیح کار کنند. همچنین، توســـعه و بهینه‌ســـازی مدل‌های موجود به‌منظور تطبیق با تکنیک‌های جدید پولشویی بسیار ضروری است.

۴- حمایت از تحقیقات و توسعه فناوری: حمایت از تحقیقات علمی و توسـعه فناوری در زمینه یادگیری ماشـینی می‌تواند به ارتقای کارایی سیستم‌های نظارتی و پیشگیری از پولشویی کمک کند. سیاست‌گذاران و نهادهای مالی باید به‌طور مداوم از جدیدترین دسـتاوردهای علمی در این حوزه بهره‌برداری کنند.

۵- همکاری‌های بین‌المللی: برای مقابله با پولشویی در تراکنش‌های رمزارزی، همکاری‌های بین‌المللی و تبادل اطلاعات میان نهادهای مالی و نظارتی ایران و دیگر کشـورها ضـروری اسـت. تدوین اسـتانداردهای بین‌المللی برای شناسایی و جلوگیری از جرایم مالی در فضای رمزارزها می‌تواند به کارآمدی این فرآیند کمک کند.

مراجع

[۱] ع. محمودی, ا. احمدی ,و ر. علی پور, "تأثیر قانون مبارزه با پول‌شویی بر کشف جرم منشأ و پیشگیری از فعالیت‌های اقتصادی مجرمانه در ایران "پژوهشنامه حقوق کیفری , no. Online First, Oct. 2023, ۲۰۲۳.۲۵۱۳۳.۲۳۹۶/jol.۱۰.۲۲۱۲۴https://doi.org/

[۲] م. مددی و س. قماشی, "جستاری در پول‌شویی از طریق ارزهای رمزنگاری شده" مطالعات حقوق کیفری و جرم شناسی , vol. 51, no. 2, Feb. 2022, ۲۰۲۳.۲۵۱۳۳.۲۳۹۶/jol.۱۰.۲۲۱۲۴https://doi.org/

[۳] ش. عبدالهی قهفرخی, ب. پاکزاد, ح. عالی پور و م. الهی منش, "پیشگیری از پولشویی الکترونیکی: رویکرد دفاعی و رویکرد هجومی.https://doi.org/10.22034/jclc.2021.290298. 1510," JCLC, vol. 9, no. 18, Jan. 2022

[۴] م. حاجی ده‌آبادی و م. خاقانی‌اصفهانی، "گونه‌شناسی سیاست کیفری فنی در قبال جرم رمزنگاری اطلاعات از منظر آزادی‌گرایی و امنیت‌گرایی،" آموزه‌های حقوق کیفری، vol. 10, no. 5, 1392. https://dorl.net/dor/20.1001.1.22519351.1392.10.5.4.0.

[5] Dreżewski, J. Sepielak, and W. Filipkowski, "The application of social network analysis algorithms in a system supporting money laundering detection," *Information Sciences*, vol. 295, pp. 18–32, Feb. 2015. https://doi.org/10.1016/j.ins.2014.10.015.

[6] Y. Dorogy and V. Kolisnichenko, "Blockchain transaction analysis: A comprehensive review of applications, tasks and methods," *System Research and Information Technologies*, no. 4, pp. 37–53, 2023https://doi.org/10.20535/srit.2308-8893.2023.4.03

[7] Y. Zhang and P. Trubey, "Machine learning and sampling scheme: An empirical study of money laundering detection," *Computational Economics*, vol. 54, no. 3, pp. 1043–1063, 2018 https://doi.org/10.1007/s10614-018-9864-z.

[8] S. R. Sandeep, S. Ahamad, D. Saxena, K. Srivastava, S. Jaiswal, and A. Bora, "To understand the relationship between machine learning and artificial intelligence in large and diversified business organisations," *Materials Today: Proceedings*, vol. 56, pp. 2082–2086, 2022. https://doi.org/10.1016/j.matpr.2021.11.409

[9] J. Lorenz, M. I. Silva, D. Aparício, J. T. Ascensão, and P. Bizarro, "Machine learning methods to detect money

laundering in the bitcoin blockchain in the presence of label scarcity," in *Proceedings of the First ACM International Conference on AI in Finance (ICAIF '20)*, 2020. https://doi.org/10.1145/3383455.3422549

[10] M. Ramalingam, G. C. Selvi, N. Victor, R. Chengoden, S. Bhattacharya, P. K. R. Maddikunta, D. Lee, Md. J. Piran, N. Khare, G. Yenduri, and T. R. Gadekallu, "A comprehensive analysis of blockchain applications for securing computer vision systems," *IEEE Access*, vol. 11, pp. 107309–107330, 2023. https://doi.org/10.1109/access.2023.3319089

[11] O. Japinye, "Integrating machine learning in anti-money laundering through crypto: A comprehensive performance review," European Journal of Accounting, Auditing and Finance Research, vol. 12, no. 4, pp. 54–80, 2024. https://doi.org/10.37745/ejaafr.2013/vol12n45480

[12] E. Petterson Ruiz, J. Angelis, and et al., "Combating money laundering with machine learning – Applicability of supervised-learning algorithms at cryptocurrency exchanges," *Journal of Money Laundering Control*, vol. 25, no. 4, pp. 766–778, 2021. https://doi.org/10.1108/jmlc-09-2021-0106

[13] H. Almeida, P. Pinto, and A. Fernández Vilas, "A review on cryptocurrency transaction methods for money laundering," in *Proceedings of the 5th International Conference on Finance, Economics, Management and IT Business*, 2023. https://doi.org/10.5220/0011993300003494

[14] C. Wronka, "Money laundering through cryptocurrencies - Analysis of the phenomenon and appropriate prevention measures," *Journal of Money Laundering Control*, vol. 25, no. 1, pp. 79–94, 2021. doi: [10.1108/jmlc-02-2021-0017](https://doi.org/10.1108/jmlc-02-2021-0017).

[15] F. M. J. Teichmann and M.-C. Falker, "Money laundering via cryptocurrencies – Potential solutions from Liechtenstein," *Journal of Money Laundering Control*, vol. 24, no. 1, pp. 91–101, 2020. doi: 10.1108/jmlc-04-2020-0041

[16] G. L. Gray, "An exploration of the money laundering associated with the Bitfinex Bitcoin hack," *Journal of Emerging Technologies in Accounting*, vol. 21, no. 1, pp. 43–57, 2024. doi: 10.2308/jeta-2023-017

[17] B. N. Pambudi, I. Hidayah, and S. Fauziati, "Improving money laundering detection using optimized support vector machine," in *2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2019. doi: 10.1109/isriti48646.2019.9034655.

[18] A. Gupta, D. N. Dwivedi, J. Shah, and A. Jain, "Data quality issues leading to sub-optimal machine learning for money laundering models," Journal of Money Laundering Control, vol. 25, no. 3, pp. 551–555, 2021. doi: 10.1108/jmlc-05-2021-0049.

[19] Y. Suga, M. Shimaoka, M. Sato, and H. Nakajima, "Securing cryptocurrency exchange: Building up standard from huge failures," in *Lecture Notes in Computer Science*, pp. 254–270, 2020. doi: 10.1007/978-3-030-54455-3_19.

[۲۰] زهرا ایزدی و نسترن ارزانیان، «پیشگیری از جرایم پولشویی و کلاهبرداری در بستر استفاده از رمزارزهای جهانی»، فصلنامه رهیافت پیشگیری از جرم، دوره ۲، شماره ۱، صفحات ۱-۱۴، ۱۳۹۸.

[21] N. Thoiba Singh, M. Mehra, I. Verma, N. Singh, D. Gandhi, and M. Ahmad Alladin, "Advancing crime analysis and prediction: A comprehensive exploration of machine learning applications in criminal justice," in *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, 2024. doi: 10.1109/idciot59759.2024.10467221