Combating Modern Money Laundering and Fraud through the Misuse of Financial Technologies

Amirhossein Dehghanpour[1], Fardin Shaghaghi[2]

S.D.I.L.
The SD Institute of Law Research & Study

Publisher:
Shahr-e- Danesh Research and Study Institute of Law

Article Type:
Original Research

DOI:
10.48300/jfel.2026.579831.1082

Received:
31 December 2025

Accepted:
1 March 2026

Published:
11 March 2026

Abstract

The rapid expansion of modern financial technologies (FinTech) has generated significant economic and commercial benefits. However, characteristics such as relative anonymity, high transaction speed, and cross-border accessibility have simultaneously created new and increasingly sophisticated opportunities for money laundering and fraud, thereby challenging conventional regulatory and enforcement mechanisms. This study aims to identify and analyze the challenges arising from the misuse of emerging financial technologies in financial crimes and to propose effective legislative and regulatory strategies for addressing these evolving threats. The research adopts a descriptive-analytical approach based on library research. Data were collected and analyzed through a systematic review of authoritative scholarly articles, specialized books, and relevant national and international legal instruments. The findings indicate that emerging financial technologies have significantly increased both the complexity and the scope of money laundering and fraud. Effective prevention and control of these crimes require a multidimensional strategy comprising targeted legislative reforms -such as the legal recognition of digital assets and the criminalization of technology-enabled financial misconduct - the development of adaptive regulatory frameworks, including mandatory customer due diligence (Know Your Customer (KYC)) requirements for digital platforms, and the strengthening of international cooperation. Furthermore, the strategic use of advanced technologies, including artificial intelligence and blockchain analytics, is essential for improving the detection, prevention, and investigation of financial crimes. The study concludes that combating financial crimes facilitated

1. (*Corresponding Author) PhD Student in Criminal Law and Criminology, Faculty of Law and Political Science, University of Mazandaran, Babolsar, Iran.
Amirdakl39@gmail.com
2. PhD Student in Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran.
fa.shagagi@mail.sbu.ac.ir

by financial technologies requires a comprehensive, dynamic, and coordinated framework that integrates legal modernization, intelligent regulatory oversight, enhanced international collaboration, and the strategic deployment of innovative technological tools to safeguard the integrity, transparency, and stability of the financial system.

Keywords: Modern Money Laundering, Financial Technologies (FinTech), Cryptocurrencies, Digital Supervision, Financial Security.

Funding: The author(s) received no financial support (funding, grants, and sponsorship) for the research, authorship, and/or publication of this article.

Author contributions:
Amirhossein Dehghanpour: Conceptualization, Methodology, Validation, Investigation, Writing - Original Draft, Writing - Review & Editing, Project Administration.
Fardin Shaghaghi: Formal Analysis, Investigation, Resources, Data Curation, Writing - Review & Editing.

Competing interests:
The authors declare that they have no competing interests.

Citation:
Dehghanpour, Amirhossein & Fardin Shaghaghi. (2025). Combating Modern Money Laundering and Fraud through the Misuse of Financial Technologies. *Journal of Financial and Economic Law*, 2(3): 213-242.

Extended Abstract

The rapid proliferation of emerging financial technologies has transformed the global financial services landscape while simultaneously creating sophisticated platforms for money laundering and financial fraud, thereby challenging traditional regulatory and enforcement mechanisms. Features inherent in these technologies - including the relative anonymity of transactions, the rapid execution of cross-border transfers, and the decentralized architecture of cryptocurrencies - facilitate the concealment of illicit financial proceeds and the circumvention of conventional supervisory systems. At the same time, increasingly sophisticated criminal techniques, such as transaction mixing, address obfuscation, phishing, business email compromise, digital identity forgery, and deepfake-enabled fraud, have significantly complicated the tracing of illicit financial flows, even through advanced blockchain transaction analysis. A comprehensive review of the existing literature indicates that, although individual aspects of these challenges have been examined, a substantial gap remains in developing an integrated framework that simultaneously addresses their legislative, supervisory, technological, and international dimensions. This gap is particularly evident in the Iranian legal system, where the legal status of cryptocurrencies remains uncertain and the 2018 Anti-Money Laundering Act contains no provisions specifically addressing digital assets. This legislative deficiency has facilitated criminal exploitation while limiting the availability of effective legal remedies for victims. Accordingly, this study aims to identify and analyze the challenges arising from the misuse of emerging financial technologies in money laundering and fraud and to propose comprehensive countermeasures centered on legislative reform, digital regulatory governance, and strengthened international cooperation. The research adopts a descriptive-analytical methodology based on library and documentary sources, including legal scholarship, peer-reviewed studies, domestic legislation, and international legal instruments. The findings demonstrate that emerging financial technologies have fundamentally reshaped the nature of financial crime. The defining characteristics of cryptocurrencies - including decentralization, relative anonymity, and instantaneous cross-border transferability - have substantially enhanced criminals' ability to conceal their identities and disguise the origins of illicit funds. Techniques such as transaction mixing, the use of unlicensed cryptocurrency exchanges, cryptocurrency ATM exploitation, decentralized finance platforms, and dark web marketplaces have become effective tools for laundering criminal proceeds. Typically, illicit assets are fragmented into numerous micro-transactions and repeatedly transferred through multiple wallets before being merged with other digital assets, thereby obscuring ownership trails to the extent that even sophisticated blockchain monitoring systems encounter significant difficulties in identifying the original source and ultimate destination of funds. The widespread use of anonymization technologies, including the Tor network and virtual private networks, further conceals users' identities, while methods such as exclusive cryptocurrency mining enable illicit proceeds to be converted into seemingly legitimate mining revenues. Likewise, cryptocurrency-based gambling and online gaming platforms provide additional opportunities to legitimize illicit funds while bypassing conventional anti-money laundering controls. In the sphere of fraud, cyberattacks involving phishing, identity theft, business email compromise, and AI-assisted deepfake technologies have substantially increased the effectiveness of financial deception by exploiting weaknesses in conventional authentication systems. Collectively, these developments have significantly diminished the

effectiveness of traditional investigative and supervisory approaches and necessitate a fundamental reassessment of existing regulatory strategies. The study further demonstrates that addressing these challenges requires a comprehensive and multidimensional regulatory framework. From a legislative perspective, cryptocurrencies should be explicitly incorporated within anti-money laundering legislation, while the misuse of decentralized exchanges and decentralized finance protocols should be clearly criminalized. The legal framework should also establish comprehensive procedures governing the seizure, confiscation, management, and recovery of criminal digital assets. Procedurally, judicial authorities and law enforcement agencies should be equipped with advanced blockchain analytics, artificial intelligence, and specialized cyber-forensic capabilities to improve investigative effectiveness. At the regulatory level, cryptocurrency exchanges should be required to implement robust Know Your Customer (KYC) procedures, continuous transaction monitoring, and mandatory suspicious transaction reporting. Given the inherently transnational nature of digital financial crimes, effective international cooperation is equally indispensable. Strengthening collaboration with international organizations such as the Financial Action Task Force (FATF), expanding mutual legal assistance mechanisms, and improving extradition cooperation are essential for combating cross-border financial crime. These measures are particularly significant for Iran, where FATF blacklisting and non-accession to international conventions such as the Palermo Convention continue to present substantial legal and practical challenges. The findings also highlight that emerging technologies themselves constitute an important component of the solution. Artificial intelligence and machine learning significantly enhance anti-money laundering systems by identifying complex transaction patterns, detecting anomalous financial behavior, and improving risk assessment capabilities. Existing empirical evidence indicates that AI-assisted anti-money laundering systems have reduced false-positive alerts by approximately 70% while increasing the detection of high-risk transactions by nearly 30%, thereby substantially improving regulatory efficiency. The principal contribution of this study is the development of a dynamic and integrated counter-strategy that moves beyond the fragmented approaches adopted in previous studies. This framework simultaneously integrates four complementary dimensions: targeted legislative reform, intelligent risk-based digital supervision, strategic deployment of advanced technologies for detection and prevention, and active international cooperation. By combining these interconnected dimensions within a unified conceptual framework, the proposed model addresses a significant gap in the existing literature and offers a more coherent strategy for combating technology-enabled financial crime. Overall, the findings demonstrate that as long as legal and regulatory systems continue to rely on fragmented, isolated, and reactive responses, emerging financial technologies will remain vulnerable to criminal exploitation despite their considerable economic and technological benefits. Effective prevention of technology-enabled financial crime requires an integrated governance model that combines legislative modernization, intelligent regulatory oversight, advanced technological capabilities, and sustained international cooperation. Such a comprehensive approach not only strengthens the capacity of legal systems to detect and prevent financial crimes but also enhances the integrity, transparency, and resilience of the global financial system in the digital era.

مقابله با روش‌های نوین پول‌شویی و کلاهبرداری از طریق سوءاستفاده از فناوری‌های مالی

امیرحسین دهقان‌پور[1*]، فردین شقاقی[2]

چکیده

گسترش سریع فناوری‌های مالی نوین ضمن ایجاد مزایای قابل توجه، به دلیل ویژگی‌هایی چون «ناشناسی نسبی»، «سرعت بالا» و «ماهیت فرامرزی»، بسترهای جدید و پیچیده‌ای را برای ارتکاب جرایم پول‌شویی و کلاهبرداری فراهم آورده و سازکارهای سنتی مقابله را به چالش کشیده است. هدف اصلی این پژوهش، شناسایی و تحلیل چالش‌های ناشی از سوءاستفاده از فناوری‌های نوین در جرایم مالی و ارائه راهکارهای مؤثر تقنینی ـ نظارتی برای مقابله با این تهدیدات جدید است. این پژوهش با رویکرد توصیفی ـ تحلیلی و بر پایه مطالعات کتابخانه‌ای انجام شده است. بدین منظور کتاب‌های تخصصی، مقالات علمی معتبر و اسناد حقوقی ملی و بین‌المللی مرتبط بررسی و تحلیل گردید و داده‌های پژوهش از طریق تحلیل محتوای این منابع گردآوری و تفسیر شد. یافته‌های این پژوهش نشان می‌دهد که فناوری‌های نوین مالی، پیچیدگی و گستره جرایم پول‌شویی و کلاهبرداری را به‌طور معناداری افزایش داده‌اند و مقابله کارآمد نسبت به این قبیل جرایم، مستلزم یک رویکرد چندوجهی شامل اصلاحات تقنینی هدفمند (مانند شناسایی حقوقی دارایی دیجیتال و جرم‌انگاری سوءاستفاده)، توسعه

پژوهشکدهٔ حقوق

نوع مقاله: علمی ـ پژوهشی

DOI:
10.48300/jfel.2026.579831.1082

تاریخ دریافت:
۱۰ دی ۱۴۰۴

تاریخ پذیرش:
۱۰ اسفند ۱۴۰۴

تاریخ انتشار:
۲۰ اسفند ۱۴۰۴

۱. (*نویسنده مسئول) دانشجوی دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه مازندران، بابلسر، ایران.
Amirdakl39@gmail.com

۲. دانشجوی دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.
fa.shagagi@mail.sbu.ac.ir

چهارچوب‌های نظارتی پویا (مانند الزام به احراز هویت مشتری در پلتفرم‌های دیجیتال) و تقویت همکاری‌های بین‌المللی است. همچنین بهره‌گیری از خود فناوری‌ها (مانند هوش مصنوعی و تحلیل بلاکچین) برای کشف و پیشگیری نیز ضروری است. درنتیجه مقابله مؤثر با جرایم مالی ناشی از سوءاستفاده از فناوری‌های مالی، نیازمند اتخاذ یک راهبرد جامع، پویا و هماهنگ است که شامل «به‌روزرسانی قوانین»، «پیاده‌سازی نظارت هوشمند»، «تقویت همکاری‌های بین‌المللی» و «استفاده راهبردی از ابزارهای فناورانه نوین» برای پیشگیری، شناسایی و مقابله با این جرایم می‌شود تا سلامت و یکپارچگی نظام مالی حفظ گردد.

کلیدواژه‌ها: پول‌شویی نوین، فناوری‌های مالی، رمزارزها، نظارت دیجیتال، امنیت مالی.

حامی مالی:
این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:
امیرحسین دهقان‌پور: مفهوم‌سازی، روش‌شناسی، اعتبارسنجی، تحقیق و بررسی، نوشتن ـ پیش‌نویس اصلی، نوشتن ـ بررسی و ویرایش، مدیریت پروژه.
فردین شقاقی: تحلیل، تحقیق و بررسی، منابع، نظارت بر داده‌ها، نوشتن ـ بررسی و ویرایش.

تعارض منافع:
بنابر اظهار نویسندگان این مقاله تعارض منافع ندارد.

استناددهی:
دهقان‌پور، امیرحسین و فردین شقاقی. (۱۴۰۴). ابعاد حقوقی رسیدگی به اعتراضات نزد بورس کالا در حقوق ایران (مسائل شکلی). مجله پژوهشهای حقوق مالی و اقتصادی، ۲(۳): ۲۱۳-۲۴۲.

مقدمه

ظهور و گسترش پرشتاب «فناوری‌های مالی نوین»[۳] در دهه‌های اخیر، چشم‌انداز خدمات مالی جهانی را به‌طور بنیادین دگرگون ساخته است. نوآوری‌هایی نظیر رمزارزها، فناوری بلاکچین، سیستم‌های پرداخت دیجیتال پیشرفته، هوش مصنوعی و یادگیری ماشینی، ضمن افزایش چشمگیر سرعت، شفافیت و دسترسی به خدمات مالی، پارادایم‌های سنتی این حوزه را به چالش کشیده‌اند. این تحولات که از دهه ۱۹۹۰ با گسترش اینترنت و کاهش هزینه‌های ارتباطی شتاب گرفت (مغنی و دیگران، ۱۳۹۸: ۱۸۴-۱۸۵)، اگرچه مزایای انکارناپذیری در کارایی و کاهش هزینه‌های معاملاتی به همراه داشته، اما به‌موازات آن بسترهای جدید و پیچیده‌ای را برای ارتکاب جرایم مالی، به‌ویژه «پول‌شویی» و «کلاهبرداری‌های نوین» فراهم آورده است. ویژگی‌هایی چون «قابلیت انجام تراکنش‌های ناشناس یا نیمه‌ناشناس»، «سرعت بالای انتقال وجوه در مقیاس فرامرزی» و «ساختارهای اغلب غیرمتمرکز برخی از این فناوری‌ها» به‌خصوص رمزارزها، پنهان‌سازی منشأ غیرقانونی وجوه و فرار از نظارت‌های مالی سنتی را برای مجرمان تسهیل نموده است.

ماهیت در ذات «فرامرزی» اقتصاد دیجیتال و پلتفرم‌های مالی نوین، چالش‌های شناسایی، تحقیق و تعقیب جرایم مالی را دوچندان کرده است. مجرمان با بهره‌گیری از این ویژگی می‌توانند فعالیت‌های مجرمانه خود را در حوزه‌های قضایی متعدد سازمان‌دهی کنند و از خلأها یا تفاوت‌های نظارتی میان کشورها سوءاستفاده نمایند. ساختارهای «غیرمتمرکز» و تکنیک‌های پیشرفته‌ای مانند «مخلوط‌سازی تراکنش‌ها»[۴] و «گمنام‌سازی آدرس‌ها»[۵] در بستر رمزارزها، ردیابی جریان وجوه نامشروع را حتی برای تحلیل‌های پیچیده گراف تراکنش نیز دشوار می‌سازد (عزیزی و سلیمانی، ۱۳۹۸: ۷۸؛ مددی و قماشی، ۱۴۰۰: ۵۱۰-۵۱۱). علاوه بر این روش‌های کلاهبرداری نوین با استفاده از ابزارهای سایبری مانند «فیشینگ»[۶]، «مهندسی اجتماعی»[۷] و «جعل هویت دیجیتال»[۸]، به طرز فزاینده‌ای امنیت مالی کاربران و مؤسسات را تهدید می‌کند. این مسائل با فقدان نسبی چهارچوب‌های قانونی و نظارتی جامع و هماهنگ در سطح ملی و بین‌المللی برای مدیریت ریسک‌های ناشی از این فناوری‌ها، تشدید می‌شود.

با توجه به پیچیدگی‌ها و تهدیدات نوظهور ناشی از سوءاستفاده از فناوری‌های مالی، این

3. FinTech
4. Mixing/Tumbling
5. Address Anonymization
6. Phishing
7. Social Engineering
8. Digital Identity Theft

پژوهش در پی پاسخ به این سؤال اصلی است که «چگونه می‌توان با بهره‌گیری از راهکارهای تقنینی، نظارتی و فناورانه نوین، به شیوه‌ای مؤثر با روش‌های جدید پول‌شویی و کلاهبرداری که از بستر فناوری‌های مالی سوءاستفاده می‌کنند، مقابله نمود؟» در راستای پاسخ به این سؤال، پژوهش حاضر بر فرضیات زیر استوار است:

۱- ویژگی‌های منحصربه‌فرد فناوری‌های مالی نوین (مانند ناشناسی نسبی، تمرکززدایی، سرعت و فرامرزی بودن) به‌طور معناداری پیچیدگی و گستره جرایم پول‌شویی و کلاهبرداری را افزایش داده و سازکارهای مقابله‌ای سنتی را ناکارآمد ساخته است.

۲- مقابله مؤثر با این جرایم نیازمند رویکردی چندوجهی شامل اصلاحات تقنینی هدفمند (جرم‌انگاری دقیق و تعیین مسئولیت‌ها)، توسعه چهارچوب‌های نظارتی دیجیتال پویا (مبتنی بر ریسک و فناوری) و تقویت همکاری‌های بین‌المللی است.

۳- بهره‌گیری هوشمندانه از خود فناوری‌های نوین (مانند هوش مصنوعی برای تحلیل داده‌ها، بلاکچین برای شفافیت کنترل‌شده) در کنار ابزارهای نظارتی سنتی، می‌تواند ظرفیت نظام‌های مالی برای پیشگیری، شناسایی و مقابله با این جرایم را به شکل قابل توجهی ارتقا دهد.

این پژوهش با اتخاذ روش تحقیق توصیفی ـ تحلیلی و با استفاده از منابع کتابخانه‌ای شامل کتب، مقالات علمی معتبر و اسناد حقوقی ملی و بین‌المللی، به بررسی ابعاد مختلف موضوع می‌پردازد. در ابتدا ضمن مقایسه فناوری‌های نوین مالی با ساختارهای سنتی، بسترها و ابزارهای نوین مورد استفاده در پول‌شویی و کلاهبرداری (با تمرکز بر رمزارزها، جرایم سایبری و سیستم‌های پرداخت دیجیتال) تحلیل خواهند شد. سپس راهکارهای مقابله‌ای در سه محور اصلی «اصلاحات تقنینی و به‌روزرسانی مقررات کیفری»، «توسعه و اجرای چهارچوب‌های نظارتی دیجیتال» و «تقویت همکاری‌های بین‌المللی» مورد بحث و بررسی قرار گرفته و درنهایت راهبردهای پیشگیرانه با تأکید بر نقش فناوری‌های نوین در فرایند مقابله، تبیین خواهند شد. هدف نهایی پژوهش، ارائه تصویری جامع از چالش‌ها و راهکارها و کمک به شکل‌گیری سیاست‌های مؤثرتر در برابر این پدیده مجرمانه نوظهور است.

۱- همگام‌سازی فناوری‌های نوین در مقابله با جرایم پول‌شویی و کلاهبرداری

هدف اصلی این بخش، تعیین چهارچوب‌های قانونی و نظارتی منسجم برای شناسایی الگوهای تراکنش مشکوک و پیشگیری از ارتکاب جرایم «پول‌شویی و کلاهبرداری نوین»، به همراه بهبود کارایی سیستم‌های امنیتی و کاهش هزینه‌های نظارتی از طریق تلفیق هوشمندانه فناوری‌های

نوین و ساختارهای سنتی است.

۱-۱- فناوری‌های نوین در برابر ساختارهای سنتی

امروزه فناوری مالی به‌عنوان یکی از مؤلفه‌های رشد اقتصادی در گسترش توسعه مالی و استقرار نظام اطلاع‌رسانی جهانی به شکل فزاینده‌ای نقش دارد. چنین روند رو به رشدی، زمینه تحولات شگرفی را در ساختارهای اقتصادی و نظام پولی و مالی ایجاد کرده است. صنعت تجاری و بانکی به‌عنوان یکی از پیشگامان گسترش خدمات مالی در عرصه فعالیت‌های اقتصادی، به‌سرعت تحت تأثیر تحولات فناوری‌های نوین قرار گرفته است و ایجاد موج جدیدی از فضای رقابتی گسترش بانکداری دیجیتال در میان فعالان این حوزه، بهره‌گیری گسترده از فناوری‌های روز دنیا، ارتقای کیفیت خدمات پولی و مالی و ایجاد شبکه‌های گسترده پولی و مالی، عملکرد چنین نهادهایی را متأثر ساخته است (مغنی و دیگران، ۱۳۹۸: ۱۸۴). همچنین خدمات فناوری مالی از دهه ۱۹۵۰ به‌تدریج وارد فعالیت‌های بانکی شد، استفاده از کارت‌های اعتباری در بین افراد عمومیت یافت و در دهه ۱۹۶۰ بهره‌گیری از خودپردازها شروع شد. تبادل الکترونیکی سهام در دهه ۱۹۷۰، به بازارهای مالی راه پیدا کرد و گسترش فناوری‌های شبکه‌ای و پیشرفت در ثبت اطلاعات و سامانه‌های داده‌ای در دهه ۱۹۸۰ گسترش یافت. این روند در دهه ۱۹۹۰ با گسترش تجارت الکترونیکی، توسعه خدمات مالی مبتنی بر اینترنت و افزایش مشارکت سرمایه‌گذاران خرد در معاملات برخط سهام شتاب بیشتری گرفت. مجموع این تحولات، بیانگر گسترش مستمر و تحول بنیادین خدمات مبتنی بر فناوری‌های مالی در دهه‌های اخیر است (مغنی و دیگران، ۱۳۹۸: ۱۸۵).

تفاوت‌های بیان‌شده، به‌طور مستقیم بر شیوه‌های ارتکاب جرایم مالی نیز تأثیرگذار است. به‌عنوان مثال در حوزه پول‌شویی، فناوری‌های نوین امکان انجام تراکنش‌های دیجیتال ناشناس با استفاده از روش‌هایی مانند «مخلوط‌سازی تراکنش‌ها» و «گمنام‌سازی آدرس‌ها» را فراهم می‌آورند، در حالی که جرایم سنتی مانند «جعل و تقلب در اسناد یا استفاده از روش‌های سنتی تجاری»، گرچه هنوز کاربرد دارند، اما به دلیل فناوری و زنجیره‌های فیزیکی کمتر کارآمد هستند. از سوی دیگر، فناوری‌هایی نظیر «بلاکچین» با ارائه یک دفتر کل غیرقابل تغییر و شفاف می‌توانند در تشخیص و پیشگیری از جرایم مالی، مؤثر واقع شوند. همچنین ابزارهای نوین همچون «هوش مصنوعی»، با تحلیل داده‌های وسیع و الگوهای پیچیده و غیرعادی، به‌سرعت فعالیت‌های مشکوک را شناسایی کرده و امکان پاسخگویی پیشگیرانه را فراهم می‌آورند.

درنهایت تلفیق هوشمندانه ویژگی‌های هر دو دسته فناوری، ضمن بهره‌مندی از مزایای سرعت و نوآوری فناوری‌های مدرن، می‌تواند از طریق چهارچوب‌های قانونی و نظارتی جامع، یک سیستم مالی امن‌تر و کارآمدتر را در برابر جرایم مالی نظیر پول‌شویی و کلاهبرداری ایجاد

کند. به‌عنوان مثال ترکیب «بلاکچین» با «سیستم‌های نظارتی سنتی»، می‌تواند شفافیت و ردیابی تراکنش‌ها را افزایش دهد، به‌گونه‌ای که تمامی معاملات در یک «دفتر کل غیرقابل تغییر»، ثبت شوند و «نهادهای نظارتی» بتوانند هرگونه رفتار مشکوک را به‌سرعت شناسایی کنند. همچنین بهره‌گیری از «الگوریتم‌های یادگیری ماشین» در کنار «پایگاه‌های داده مالی سنتی»، می‌تواند الگوهای غیرعادی را در تراکنش‌های بانکی تشخیص داده و در مراحل اولیه از وقوع تخلفات مالی به‌وسیله ضابطان اقتصادی جلوگیری کند. از سوی دیگر ترکیب راهکارهای امنیت سایبری مدرن، نظیر «احراز هویت چندعاملی» و «رمزگذاری پیشرفته»، با «پروتکل‌های سنتی نظارت بر حساب‌ها» می‌تواند از کلاهبرداری‌های مالی جلوگیری کند. برای مثال بانک‌هایی که علاوه بر نظارت انسانی، از ابزارهای پیشرفته بیومتریک (مانند اسکن اثرانگشت یا تشخیص چهره) استفاده می‌کنند، توانسته‌اند به میزان قابل توجهی از جعل هویت و سرقت اطلاعات جلوگیری کنند. درنتیجه ایجاد یک سیستم مالی ترکیبی که هم از قدرت نظارتی فناوری‌های سنتی و هم از ظرفیت تحلیل و سرعت فناوری‌های نوین بهره می‌برد، می‌تواند نه‌تنها امنیت مالی را افزایش دهد، بلکه با کاهش هزینه‌های نظارتی و افزایش دقت در شناسایی جرایم، کارآمدی کلی این سیستم را بهبود بخشد.

۱-۲- نوآوری‌های دیجیتال و تحول بازار مالی: بستر ظهور پول‌شویی و کلاهبرداری نوین

پیشرفت‌های سریع در فناوری‌های دیجیتال، تحولی بنیادین در بازارهای مالی جهان ایجاد کرده است. این تحولات، ضمن ارائه فرصت‌های نوآورانه برای سهولت معاملات و دسترسی گسترده‌تر به خدمات مالی، زمینه‌ساز ظهور روش‌های جدیدی برای ارتکاب جرایم مالی و اقتصادی نیز شده‌اند؛ به عبارت دیگر ظهور ابزارهای نوین در حوزه بازارهای مالی همچون «رمزارزها»، «سیستم‌های پرداخت دیجیتال»، «بانکداری اینترنتی و موبایلی»، «پلتفرم‌های وام‌دهی آنلاین» و «کاربرد هوش مصنوعی و داده‌کاوی»، از طرفی موجب بهبود کارایی و شفافیت سیستم‌های مالی شده است و از سوی دیگر خود، به دلیل ناشناسی و پیچیدگی‌های فنی، زمینه‌ساز ارتکاب جرایمی مانند پول‌شویی و کلاهبرداری نوین اینترنتی نیز گردیده است.

در فضای نوین دیجیتالی، از یک سو متخلفان سایبری با بهره‌برداری از نقاط ضعف موجود در روش‌های «احراز هویت سنتی»، «رمزنگاری ناکافی داده‌های حساس»، «به‌روزرسانی مستمر سیستم‌ها» و «آسیب‌پذیری شبکه‌های اجتماعی»، از متدهایی نظیر «فیشینگ، مهندسی اجتماعی و ایجاد هویت‌های جعلی» استفاده کرده و با استفاده از فناوری‌های پیشرفته هوش مصنوعی، مانند دیپ‌فیک‌ها و شبیه‌سازی صدا، دسترسی غیرمجاز به اطلاعات حساس را تسهیل می‌کنند. افزون بر این ساختار غیرمتمرکز پلتفرم‌های وام‌دهی همتا به همتا و تأمین مالی

جمعی، به دلیل امکان انجام تراکنش‌های کوچک و متعدد و بهره‌برداری از تفاوت‌های نظارتی بین حوزه‌های قضایی، مجرمان را قادر می‌سازد تا وجوه غیرقانونی را از طریق فرایندهای ساختاری پنهان نمایند.

در کنار این موارد، پیشرفت‌های چشمگیر در فناوری‌های هوش مصنوعی و داده‌کاوی، منجر به تحولاتی اساسی در شیوه‌های مبارزه با جرایم مالی و اقتصادی شده است، به‌طوری که الگوریتم‌های یادگیری ماشین با تحلیل حجم عظیم داده‌های ساختاریافته و منسجم و حتی غیرمنسجم، الگوهای تراکنش، رفتار مشتریان و ارتباطات شبکه‌ای را با دقت بررسی و ناهنجاری‌های مشکوک را شناسایی می‌کنند. لذا در مواجهه با این تهدیدات چندوجهی، مؤسسات مالی ملزم به به‌روزرسانی مستمر زیرساخت‌های نظارتی و امنیتی، تقویت پروتکل‌های احراز هویت فردی و ایجاد همکاری‌های گسترده، میان نهادهای ملی و بین‌المللی به همراه بهره‌گیری از داده‌های با کیفیت و به‌خصوص بی‌طرف، جهت آموزش مدل‌های هوش مصنوعی هستند تا ضمن ارائه خدمات مالی کاربرپسند، سلامت و یکپارچگی بازارهای مالی را در برابر حملات پیچیده و ناهمگون الکترونیکی حفظ کنند.

۲- ابزارها و تکنیک‌های نوین بهره‌برداری در جرایم پول‌شویی و کلاهبرداری

این نوشتار به بررسی سه مبحث اصلی در زمینه پول‌شویی و جرایم سایبری می‌پردازد. نخست، سوءاستفاده از رمزارزها در پول‌شویی از طریق تکنیک‌های مخلوط‌سازی و گمنام‌سازی تراکنش‌ها تحلیل می‌شود. سپس جرایم سایبری و کلاهبرداری‌های اینترنتی، ازجمله فیشینگ و جعل هویت، با تأکید بر پیشگیری و مقابله بررسی می‌گردد. درنهایت نقش سیستم‌های پرداخت دیجیتال در تسهیل پول‌شویی و چالش‌های نظارتی مرتبط با آن مورد ارزیابی قرار می‌گیرد. هدف این نوشتار، ارائه درکی جامع از روش‌های نوین این جرایم و پیشنهاد راهکارهای پیشگیرانه است.

۲-۱- سوءاستفاده از رمزارزها در پول‌شویی: مخلوط‌سازی تراکنش‌ها و گمنام‌سازی آدرس‌ها

با ظهور فناوری‌های نوین در حوزه رمزارزها، سازکارهای پول‌شویی از طریق «مخلوط‌سازی تراکنش‌ها» و «گمنام‌سازی آدرس‌ها» به‌شدت پیچیده و چندلایه شده است. در این فرایند، ارزهای دیجیتال ابتدا به واحدهای خرد تبدیل شده و سپس در قالب تراکنش‌های متعدد، به‌گونه‌ای با ارزهای سایر افراد ترکیب می‌شوند که ردپای انتقال وجه به‌طور کامل از بین برود. علاوه بر این استفاده از پروتکل‌های همکاری مشترک و فناوری‌های رمزنگاری پیشرفته در کنار به‌کارگیری رمزارزهای حریم خصوصی، اطلاعات مربوط به مبدأ و مقصد تراکنش‌ها را به‌صورت چندگانه پنهان می‌کند؛ به‌طوری که حتی «تحلیل‌های گراف تراکنش» نیز قادر به تشخیص زنجیره واقعی انتقال وجوه نخواهند بود.

سازکارهای متفاوتی وجود دارد که باعث می‌شود تحلیل گراف تراکنش، کمتر مؤثر واقع شود و غیرقابل تشخیص باشد. یکی از این سازکارها، «مخلوط‌سازی» است که به‌صورت «گسترده و وابسته» صورت می‌گیرد و فقط متعلق به رمزارزها و بیت‌کوین نیست (عزیزی و سلیمانی، ۱۳۹۸: ۷۸). در روش «مخلوط کردن بیت‌کوین»[۹]، ارزهای رمزنگاری‌شده افراد مختلف به واحدهای کوچک‌تری تبدیل شده و پس از ترکیب با یکدیگر و انجام تراکنش‌های متعدد، به آدرس‌های مورد نظر این افراد ارسال می‌شود؛ به عبارت دیگر در این فرایند، ارزهای رمزنگاری‌شده هر شخص به سرویس ناشناسی ارسال شده و با پول‌های اشخاص دیگر ترکیب شده و سپس به افراد بازگردانده می‌شود (Ruffing, 2014: 357). در این پروتکل، تمامی شرکت‌کنندگان از طریق کانال‌های پرداختی، بیت‌کوین‌های تحت مالکیت خود را به آدرس معینی ارسال کرده و مقدار برابری از بیت‌کوین‌های افراد دیگر در شبکه را دریافت می‌کنند. این فرایند، مفهوم «ردپای مالکیت» را برای همه از بین می‌برد؛ به‌طوری‌که شرکت‌کنندگان و پایشگران از اینکه بیت‌کوین‌ها از چه کسانی و به چه کسانی منتقل شده است، مطلع نمی‌شوند (مددی و قماشی، ۱۴۰۰: ۵۱۰).

یکی از راه‌های کنترل دسترسی در فضای مجازی، «پایش آدرس‌های آی‌پی[۱۰] مربوط به کاربران» و «تخمین محدوده تقریبی جغرافیایی آنها» و «پیگیری اتصالات مشکوک» است. چراکه آی‌پی درواقع یک شماره شناسایی یکتا برای برقراری یک ارتباط تحت شبکه است و از طریق آنها، دستگاه‌های مختلف از هم بازشناخته می‌شوند. به‌منظور ناشناس‌سازی آدرس کاربران در شبکه بیت‌کوین، از ابزارهایی چون مرورگر «تور[۱۱]» و «وی‌پی‌ان» استفاده می‌شود. ابزارهای مزبور، به یک شخص امکان می‌دهد تا وانمود کند در مکان دیگری یا در قلمرو حقوقی دیگری اقامت دارد یا اینکه به فرد اجازه می‌دهد که چندین حساب کاربری بدون قابلیت انتساب به خود را ایجاد کند (مددی و قماشی، ۱۴۰۰: ۵۱۰-۵۱۱).

ازجمله سایر مواردی که موجب سوءاستفاده از رمزارزها می‌شود، روش «استخراج انحصاری» و همچنین «مخلوط‌سازی غیرمتمرکز» است. روش استخراج انحصاری، نوعی تبانی بین آغازکننده تراکنش و یک استخراج‌گر است. در این روش، تبهکاران مقداری بیت‌کوین را برای استخراج‌گر انحصاری خود که به‌طور کامل بر تمام فعالیت‌های آن کنترل دارند، ارسال می‌کنند و

---

9. Bitcoin Mixing
10. IP

۱۱. مرورگر تور «Tor»، ابزاری است که با استفاده از رمزگذاری چندلایه (onion routing) و مسیریابی ترافیک، هویت و موقعیت کاربران را مخفی می‌کند. این سیستم علاوه بر دور زدن سانسور و محافظت از حریم خصوصی، امکان دسترسی به سرویس‌های onion در وب تاریک را فراهم می‌کند و با پاک کردن خودکار تاریخچه مرور و رمزگشایی مرحله‌ای داده‌ها، ردیابی فعالیت‌های آنلاین مانند دانلودها، پیام‌ها و بازدیدهای وب‌سایت را تقریباً غیرممکن می‌سازد.

از آن استخراج‌گر می‌خواهند که هزینه تراکنش بالایی را جهت تأیید این تراکنش تعیین کند. پس از استخراج تراکنش مزبور، هزینه تراکنش تعیین‌شده به استخراج‌گر پرداخت می‌شود و به‌نوعی وجوه ناشی از پول‌شویی به وجوه ناشی از استخراج تغییر ماهیت می‌دهند و به یک دارایی کاملاً مشروع و قانونی بدل می‌شوند (Strehle, 2020: 6).

۲-۲- جرایم سایبری و کلاهبرداری‌های اینترنتی: الگوها و راهبردهای نفوذ

در چهارچوب موضوع «جرایم سایبری و کلاهبرداری‌های اینترنتی»، بررسی تاریخچه وقوع کلاهبرداری اینترنتی در ایران نشان می‌دهد که با توجه به محدودیت‌های اولیه کاربرد کامپیوتر و اینترنت تا دهه ۱۳۷۰، سابقه جرایم اینترنتی به‌نسبت کوتاه بوده است؛ به‌طوری که وقوع جرم کامپیوتری به‌تدریج از دهه ۱۳۷۰ آغاز شده است، اما آمار دقیقی در این زمینه موجود نیست (خرم‌آبادی، ۱۳۸۴: ١٤). از سوی دیگر مقابله مؤثر با جرایم سایبری نیازمند رعایت استانداردهای فنی و اخلاق حرفه‌ای در استفاده از فناوری‌های نوین است، به‌طوری که ارائه آموزش‌های تخصصی جهت تبیین تدابیر امنیتی و اصول اخلاق شغلی، به‌ویژه در مواجهه با گروه‌های آسیب‌پذیر مانند نوجوانان، از اهمیت ویژه‌ای برخوردار است (انصاری و میلانی، ۱۳۹۵: ۱۵۵).

سیاست جنایی که شامل دو مؤلفه «پیشگیری از ارتکاب جرم» و «پاسخ‌دهی به بزهکاران» است، به همراه وجود «نهاد ناظر» و «شفافیت اطلاعاتی» در بازارهای مالی، نقش حیاتی در جلوگیری از تقلب و جبران خسارت به سرمایه‌گذاران دارد (دهقان‌پور، ۱۴۰۲: ۱۳). افزون بر این نقش رسانه‌های جمعی در آگاه‌سازی عمومی درباره پیامدهای ناگوار جرایم سایبری و طراحی الگوهای رفتاری پیشگیرانه، از مهم‌ترین راهبردها در مقابله با کلاهبرداری اینترنتی به شمار می‌آید (دیندار فرکوش، ۱۳۸۸: ۴۰-۴۱). به‌علاوه سیاست جنایی مشارکتی که با ادغام نقش جامعه مدنی و نهادهای دولتی مانند پلیس، سازمان زندان‌ها و دستگاه قضایی در مراحل کشف جرم، تعقیب دادرسی و اجرای حکم عمل می‌کند، می‌تواند الگوی موفقی برای مقابله با این جرایم محسوب شود (لازرژ، ۱۳۹۰: ٦١؛ باصری، ۱۳۸۷: ۳۷).

با گسترش فناوری‌های دیجیتال و اینترنت، جرایم سایبری و کلاهبرداری‌های اینترنتی به چالشی جدی برای امنیت اطلاعات تبدیل شده‌اند؛ مهاجمان از روش‌های پیچیده و نوینی همچون فیشینگ به همراه جعل هویت و سازش ایمیل تجاری برای تحصیل اطلاعات حساس استفاده می‌کنند. در حالی که «کلاهبرداری‌های مبتنی بر روابط عاطفی (مانند کلاهبرداری‌های عاشقانه و مبتنی بر اعتماد)» و نیز «کلاهبرداری و فریب‌های مالی (شامل سرمایه‌گذاری‌های آنلاین ساختگی، کلاهبرداری‌های کارت اعتباری و سرقت هویت)»، خسارات

مالی و روانی گسترده‌ای به همراه دارند. افزون بر این اَشکال نوین کلاهبرداری، همچون کلاهبرداری‌های خیریه، حراج‌های آنلاین، کلاهبرداری بلیت اینترنتی و کلاهبرداری پیش‌پرداخت به همراه حملات فنی نظیر، کلیک فریبنده، رمزنگاری پنهانی و حملات باج‌افزاری، تنوع و تکامل تهدیدات سایبری را نشان می‌دهد؛ ولی در مواجهه با این تهدیدات، چالش‌های امنیتی فردی ازجمله خطاهای انسانی و گذرواژه‌های ضعیف و مشکلات سازمانی مانند کمبود متخصصان، تهدیدات داخلی، آسیب‌پذیری‌های زنجیره تأمین و محدودیت‌های بودجه، نیازمند راهکارهای چندجانبه و به‌روز است که از طریق تقویت آگاهی و آموزش کاربران، به‌کارگیری فناوری‌های نوین امنیتی مانند سیستم‌های تشخیص نفوذ مبتنی بر هوش مصنوعی، احراز هویت چندعاملی و رمزنگاری پیشرفته و ایجاد همکاری‌های بین‌المللی و چهارچوب‌های قانونی مناسب می‌توان آنها را مدیریت کرد.

در راستای تحلیل جامع تهدیدات و کلاهبرداری‌های سایبری مطرح‌شده در متن، جدول زیر به‌عنوان یک ابزار تحلیلی نوین ارائه شده که در آن به بررسی سامانمند روش‌های متنوع کلاهبرداری اینترنتی پرداخته شده است.

الگوهای کلاهبرداری اینترنتی و راهکارهای پیشگیری کلیدی

روش‌های نوین کلاهبرداری اینترنتی	شرح مختصر	نکاتی برای پیشگیری کلیدی
فیشینگ	تلاش برای به دست آوردن اطلاعات حساس از طریق ارتباطات فریبنده	بررسی آدرس ایمیل و URL، عدم کلیک بر روی لینک‌های مشکوک، عدم ارائه اطلاعات شخصی از طریق ایمیل
کلاهبرداری عاشقانه	ایجاد روابط عاطفی جعلی آنلاین برای اخاذی پول یا اطلاعات	احتیاط در مورد افرادی که خیلی زود ابراز علاقه می‌کنند، عدم ارسال پول به افرادی که ملاقات نکرده‌اید، تحقیق در مورد رزومه و پروفایل
کلاهبرداری سرمایه‌گذاری آنلاین	طرح‌هایی برای فریب افراد، به خرید سرمایه‌گذاری‌های جعلی	مراقب وعده‌های بازده بالا و ریسک کم بودن، تحقیق کردن از مشاوران ثبت‌شده و وکلا
سرقت هویت	سرقت اطلاعات برای جعل هویت	محافظت از شماره تأمین اجتماعی و سایر اطلاعات شخصی، استفاده از احراز هویت چندعاملی

کلاهبرداری خیریه	درخواست کمک مالی برای اهداف خیر ساختگی	تحقیق در مورد سازمان‌های خیریه قبل از اهدای پول، مراقب درخواست‌های فوری بودن
کلاهبرداری بلیت اینترنتی	فروش بلیت‌های جعلی یا تحویل‌نشده	از فروشندگان رسمی یا مجاز خرید کردن، مراقب قیمت‌های بسیار پایین بودن
کلاهبرداری پیش‌پرداخت	درخواست پول در ازای وعده مبلغ بیشتر در آینده	مراقب پیشنهادهای وسوسه‌انگیز بودن، به افراد ناشناس پول ارسال نکردن
فارمینگ	هدایت ترافیک وب‌سایت به سایت‌های جعلی	استفاده از HTTPS، مراقب آدرس وب‌سایت بودن
رمزنگاری پنهانی	استفاده مخفیانه از منابع قربانی برای استخراج ارز دیجیتال	استفاده از نرم‌افزار امنیتی، نظارت بر عملکرد دستگاه
حملات باج‌افزاری	رمزگذاری داده‌ها و درخواست باج	پشتیبان‌گیری منظم از داده‌ها، به‌روز نگه داشتن نرم‌افزار، مراقب پیوست‌های ایمیل بودن

۲-۳- سیستم‌های پرداخت دیجیتال: زیرساخت انتقال مالی در پول‌شویی

پول‌شویی، فرایندی پیچیده و چندوجهی است که هدف آن پنهان کردن منشأ غیرقانونی عواید حاصل از جرم و مشروع جلوه دادن آنها است. این فعالیت مخرب، نه‌تنها سلامت نظام‌های مالی را تهدید می‌کند، بلکه پیامدهای گسترده‌تری برای اقتصاد و جامعه به‌طور کلی دارد. در دنیای امروز، سیستم‌های پرداخت دیجیتال به‌عنوان شریان‌های اصلی اقتصاد جهانی، نقش حیاتی در تسهیل تجارت و تبادلات مالی ایفا می‌کنند. سرعت، سهولت و دسترسی‌پذیری این سیستم‌ها، آنها را به ابزاری قدرتمند برای افراد و کسب‌وکارها تبدیل کرده است. با این حال همین ویژگی‌ها، سیستم‌های پرداخت دیجیتال را به بستری جذاب برای مجرمان و سازمان‌های تبهکار تبدیل کرده است تا از آنها به‌عنوان زیرساخت‌های انتقال مالی در عملیات پول‌شویی استفاده کنند.

یکی از بسترهای پول‌شویی از طریق ارزهای رمزنگاری‌شده، «صرافی‌های غیرمجاز» هستند. در صرافی‌هایی که از مقررات مربوط به مقابله با پول‌شویی پیروی نمی‌کنند، فرایند احراز هویت کاربران، چندان دقیق صورت نمی‌پذیرد که این مسئله سبب پنهان ماندن «مشخصات معامله‌گر» می‌شود. در پرتو عدم شناسایی هویت کاربران، این امکان فراهم می‌آید که ارزهای رمزنگاری‌شده بارها و بارها در بازارهای مختلف معامله شده و پس از واریز به صرافی‌های غیرقانونی در خرید ارزهای دیگر از آنها استفاده شود. همچنین «قمار و بازی‌های آنلاین» از طریق سایت‌هایی که بیت‌کوین یا سایر ارزهای رمزنگاری‌شده را قبول می‌کنند، یکی دیگر از

روش‌هایی است که در طرح‌های پول‌شویی از طریق ارزهای رمزنگاری‌شده استفاده می‌شود، چراکه این سایت‌ها در اصل از قوانین مقابله با پول‌شویی پیروی ندارند و نظارت خاصی نیز بر هویت افراد صورت نمی‌پذیرد و خلاف‌کاران می‌توانند به‌واسطه فضای فراهم‌شده، پول‌های کثیف خود را به حساب سایت‌های شرط‌بندی انتقال دهند و سپس در بستری امن که این سایت‌ها فراهم کرده‌اند، پس از چند روز پول کثیف خود را از سایت قمار خارج و به حساب خود منتقل کنند (مددی و قماشی، ۱۴۰۰: ۵۱۲).

حدود ۸۰۰۰ دستگاه خودپرداز بیت‌کوین در سراسر جهان وجود دارد و امکان معامله بیت‌کوین را برای افراد فراهم آورده‌اند. دستگاه خودپرداز بیت‌کوین، این امکان را فراهم آورده است که افراد با پول‌های رایج یا کارت‌های اعتباری، بیت‌کوین تهیه کنند. در این روش، افراد پس از وارد کردن آدرس کیف پول خود یا هر کس دیگری و واریز کردن قیمت بیت‌کوین، می‌توانند بیت‌کوین خریداری شده را در کیف پول خود مشاهده کنند. در این روش، «هویت خریدار» نامشخص باقی می‌ماند و مجرمان می‌توانند از نقاط ضعف خودپرداز ارزهای رمزنگاری‌شده، برای استفاده از خطرهای مربوط به پول‌شویی سوءاستفاده کنند. به‌عنوان نمونه در یکی از پرونده‌های پول‌شویی از طریق دستگاه‌های خودپرداز بیت‌کوین، پلیس اسپانیا از کشف یک شبکه سازمان‌یافته و دستگیری هشت نفر از اتباع اسپانیا و آمریکای لاتین خبر داد. بر اساس گزارش‌ها، اعضای این شبکه با بهره‌گیری از ۹ شرکت، حدود ۹ میلیون یورو را برای قاچاقچیان مواد مخدر در کلمبیا و چند کشور دیگر جابه‌جا کرده بودند. در این شیوه، وجوه نقد پس از تبدیل به بیت‌کوین از طریق دستگاه‌های خودپرداز، به کیف‌پول‌های دیجیتالی منتقل و بلافاصله به مؤسسه‌ای ارسال می‌شد که به‌طور مستقیم تحت کنترل شبکه‌های قاچاق مواد مخدر کلمبیا قرار داشت. درنهایت دریافت‌کنندگان وجوه با مراجعه به صرافی‌های برخط ارزهای رمزنگاری‌شده، بیت‌کوین‌ها را به سایر ارزها یا پول رایج تبدیل می‌کردند (Castor, 2019).

گسترش خودپردازهای بیت‌کوین به‌عنوان کانالی برای تبدیل نقدینگی غیرقانونی به رمزارزها، چالش‌های بی‌سابقه‌ای در مبارزه با پول‌شویی ایجاد کرده است. گزارش‌های سال ۲۰۲۴ نشان می‌دهد ٪۱٫۲ تراکنش‌های خودپردازهای «کریپتو» مرتبط با فعالیت‌های مجرمانه است، رقمی که دو برابر میانگین جهانی این صنعت محاسبه شده است. نمونه‌های عملیاتی، مانند کشف شبکه ۹ میلیون یورویی پول‌شویی در اسپانیا و پرونده ۲٫۶ میلیون پوندی انگلیس در سال ۲۰۲۴، نشانگر سوءاستفاده از نقاط کور نظارتی مانند ناشناس ماندن هویت کاربران است.

۳- راهکارهای جامع مقابله با پول‌شویی و کلاهبرداری‌های نوین

مطابق با این اصل که «پول، شریان حیاتی جرم است»، مجرمان همواره می‌توانند دوباره سر

برآورده و به ارتکاب جرایم خود ادامه دهند. وجوهی که از فعالیت‌های غیرقانونی به دست می‌آیند، می‌توانند برای تأمین مالی و گسترش جرایم مورد استفاده قرار گیرند و به این ترتیب جرم را توسعه داده و سازمان‌یافته‌تر کنند. پیشرفت جرایم از نظر سازمان‌دهی، شیوه‌های عملیاتی و دامنه فعالیت، مشکلات جدی برای جامعه ایجاد می‌کند. به‌عنوان مثال قاچاق مواد مخدر نه‌تنها کاهش نمی‌یابد، بلکه روزبه‌روز به فعالیت‌های آن افزوده می‌شود. این اصطلاح برای اولین بار توسط روزنامه‌ها در گزارش رسوایی واترگیت مربوط به رئیس‌جمهور ریچارد نیکسون در سال ۱۹۷۳ استفاده شد (Syahda et al., 2024: 224). بر اساس برخی منابع دولتی، سالانه بین ۸۰۰ میلیارد تا ۲ تریلیون دلار پول نقد پول‌شویی می‌شود. این آمار در حال حاضر نیاز فوری به یافتن و اجرای راهبردهایی برای کاهش پول‌شویی تا حد امکان را نشان می‌دهد (Ujoodha & Suppiah, 2023: 1). رمزارزها به دلیل ویژگی‌هایی مانند ناشناس بودن نسبی تراکنش‌ها، غیرمتمرکز بودن، عدم وابستگی به نهادهای مالی سنتی و سهولت در انتقالات بین‌المللی، به ابزاری مناسب برای فعالیت‌های مجرمانه ازجمله پول‌شویی و کلاهبرداری تبدیل شده‌اند. برخلاف سیستم‌های بانکی که تحت قوانین سخت‌گیرانه مبارزه با پول‌شویی و تأمین مالی تروریسم فعالیت می‌کنند، بسیاری از پلتفرم‌های معاملاتی رمزارز، به‌ویژه «صرافی‌های غیرمتمرکز»، فاقد چنین نظارتی هستند و در برخی موارد حتی بدون نیاز به احراز هویت مشتری امکان انجام تراکنش را فراهم می‌کنند. مقابله با پول‌شویی از طریق ارزهای رمزگذاری‌شده نیازمند اصلاحات تقنینی، نظارت‌های دقیق دیجیتال، همکاری‌های بین‌المللی و استفاده از روش‌های نوین است که در ادامه این پژوهش مورد بررسی قرار خواهند گرفت.

۳-۱- اصلاحات تقنینی و به‌روزرسانی مقررات کیفری

پول‌شویی به‌عنوان مصداقی از جرایم اقتصادی در حقوق کیفری نوین با تکیه بر اوصاف پویایی و تنوع در روش‌های ارتکاب، نیازمند سیاست کیفری افتراقی ویژه بوده و از این رو بازنگری مداوم و تحول قوانین و مقررات ناظر بر آن ناگزیر است (قجاوند، ۱۳۹۹: ۴۶۶؛ Kartono et al., 2024: 768). در این راستا یکی از چالش‌های نوظهور که در حوزه پول‌شویی مطرح شده، ظهور ارزهای رمزنگاری‌شده است. ارزهای رمزنگاری‌شده به دلیل بدیع بودن و ساختار به‌نسبت پیچیده‌ای که دارند، تاکنون به‌صورت جامع مورد تقنین واقع نشده‌اند و در این خصوص تنها تلاش‌های اندکی در برخی کشورها صورت پذیرفته است. این موضوع سبب شده است تا یک فقدان و خلأ قانونی در این زمینه پدیدار شود و گاه افرادی که به حقوق ایشان در زمینه ارزهای رمزنگاری‌شده تعرضی صورت گرفته است، در رجوع به نهادهای قضایی و درخواست رسیدگی خود با موانع بسیاری مواجه شوند و درنتیجه به حق خود دست پیدا نکنند. افزون بر این خلأهای قانونی سبب

سوءاستفاده مجرمان نیز شده است و این افراد به ارتکاب جرایم مالی همچون پول‌شویی و کلاهبرداری می‌پردازند. شاید به همین علت است که مسئله قانون‌مندسازی بیت‌کوین واجد اهمیت بسیاری است (مددی و قماشی، ۱۴۰۰: ۵۸۲؛ Kepli & Zolhuda, 2019: 247).

یکی از راهکارهای مقابله با پول‌شویی از طریق بیت‌کوین و پذیرش این نوع ارزها، تدوین قوانین لازم برای قاعده‌مند ساختن مبادلات آن است. تدوین قوانین لازم از این جهت اهمیت دوچندان دارد که بیت‌کوین تمامی شاخه‌های حقوق را درگیر ساخته است. به‌عنوان نمونه اِعمال سازکار دریافت مالیات و یا جلوگیری از فرارهای مالیاتی در صورتی قابل‌تصور است که ارزهای مجازی همچون بیت‌کوین توسط مقنن به رسمیت شناخته شوند و از این جهت بیت‌کوین موضوع حقوق عمومی قرار می‌گیرد. این رویکرد همچنین به کشف و شناسایی جرایم کمک می‌کند؛ زیرا با جلوگیری از زیرزمینی شدن فعالیت‌های مالی، سطح شفافیت را افزایش داده و افزون بر ایجاد بازدارندگی، زمینه نظارت مؤثر، ردیابی تراکنش‌ها و کشف جرایم را نیز تسهیل می‌کند (فراتی و دیگران، ۱۳۹۹: ۶۹).

با توجه به قانون مبارزه با پول‌شویی مصوب ۱۳۹۷ و سایر قوانین کیفری ایران، مقابله با پول‌شویی از طریق رمزارزها مستلزم اصلاحات قانونی و بازنگری در برخی مقررات است تا امکان نظارت و برخورد مؤثر با این پدیده فراهم شود. از این رو نخستین اصلاح ضروری، تصریح و به رسمیت شناختن رمزارزها در قوانین کیفری ایران است. در حال حاضر وضعیت حقوقی رمزارزها در نظام حقوقی ایران به‌طور شفاف تعیین نشده و همین موضوع موجب سردرگمی در نحوه رسیدگی به جرایم مرتبط با آنها شده است؛ بنابراین لازم است تا قانونگذار با اصلاح مقررات، رمزارزها را به‌عنوان ابزار مالی تحت شمول مقررات مبارزه با پول‌شویی قرار دهد و ضوابط مشخصی برای استفاده قانونی و غیرقانونی از آنها تعیین کند. همچنین جرم‌انگاری صریح استفاده غیرقانونی از رمزارزها برای پول‌شویی و تعیین مجازات‌های متناسب با آن امری ضروری است. در حال حاضر قانون مبارزه با پول‌شویی کشور ایران (مصوب ۱۳۹۷)، بدون اشاره به رمزارزها، هرگونه تبدیل، جابه‌جایی یا انتقال عواید حاصل از جرم منشأ را مشمول جرم پول‌شویی دانسته است؛ اما با توجه به ویژگی‌های خاص رمزارزها مانند «ناشناس بودن و غیرمتمرکز بودن»، ضروری است که قانونگذار استفاده از ابزارهایی نظیر «صرافی‌های غیرمتمرکز و پروتکل‌های دیفای[۱۲]»، برای مخفی‌سازی منشأ دارایی‌ها را به‌عنوان رفتارهای مجرمانه، به‌صراحت در قوانین کیفری تعریف کند.

اهمیت پیشگیری از ارتکاب جرم پول‌شویی و کلاهبرداری در حفظ امنیت اقتصادی، اجتماعی و سیاسی کشورها ایجاب می‌کند که نه‌تنها مرتکب اصلی، بلکه تمامی اشخاص مرتبط

12. DeFi

با این جرم نیز تحت پیگرد و مجازات قرار گیرند. این موضوع چنان حائز اهمیت است که اسناد بین‌المللی موجود، برای برخی از اشخاص مرتبط با این جرم، مسئولیتی هم‌سنگ با مرتکب اصلی در نظر گرفته‌اند. به‌عنوان نمونه بند «ب» ماده ۶ کنوانسیون پالرمو، بدون اشاره مستقیم به تساوی مسئولیت معاون و شریک جرم پول‌شویی، اقداماتی نظیر مشارکت، تسهیل ارتکاب جرم، تبانی و معاونت در آن را در حکم پول‌شویی دانسته و مجازاتی برابر با مرتکب اصلی برای این افراد مقرر کرده است. اتخاذ چنین رویکردی، ناشی از تأثیر قابل‌توجه و گاه حتی فراترِ شرکا و معاونان در ارتکاب این جرم است؛ چراکه افراد وابسته به بزهکاران، اغلب نقش مغز متفکر را در اجرای پول‌شویی ایفا می‌کنند و خطر اقدامات آنها اگر بیشتر از مرتکب اصلی نباشد، بی‌شک کمتر نخواهد بود (Savla, 2001: 34).

سیاست کیفری ایران، در زمینه مقابله با پول‌شویی و کلاهبرداری از طریق رمزارزها نه‌تنها در بعد ماهوی، بلکه در بعد شکلی نیز نیازمند تحولاتی است. در بعد شکلی، چالش‌هایی همچون «کشف جرم، تعقیب کیفری، توقیف و ضبط اموال دیجیتال و چگونگی اجرای احکام کیفری در ارتباط با رمزارزها» مطرح می‌شود. یکی از مهم‌ترین مسائل، نحوه رهگیری تراکنش‌های مشکوک در بستر بلاکچین و تعیین هویت واقعی مرتکبان است، چراکه ماهیت «غیرمتمرکز» و «نیمه‌ناشناس» ارزهای دیجیتال، ردیابی آنها را دشوار می‌سازد. در این راستا باید نهادهای قضایی و ضابطین دادگستری به ابزارهای فنی و فناوری‌های نوین تحلیل داده‌های بلاکچین مجهز شوند.

در علم جرم‌یابی، صحنه جرم نقشی بسیار حیاتی دارد. در جرایم خارج از فضای مجازی در اصل به دلیل وجود دلایل مادی و فیزیکی، بررسی صحنه جرم کمک شایانی به ادامه تحقیقات و کشف جرم می‌نماید؛ اما در جرایم سایبری به دلیل دشواری در حفظ یا نبود صحنه جرم، ممکن است روند تحقیقات و تحصیل دلیل با مشکل مواجه شود. به عبارت دیگر در جرایم سایبری حفظ و بررسی صحنه جرم کاملاً متفاوت بوده و نیازمند تخصص و آموزش‌های ویژه این نوع جرایم است؛ بنابراین به‌منظور ارائه دلایل در دادگاه و اثبات اتهام، باید تدابیری به‌منظور افزایش قابلیت‌های تحصیل دلیل و مستندسازی اتخاذ شود. جرم‌یابی جرایم سایبری نسبت به جرایم عادی، پیچیدگی‌های بسیار بیشتری دارد و پلیس به‌عنوان نهاد مسئول در کشف جرایم این حوزه نیازمند همگام‌سازی توان و دانش فنی خود با پیشرفت‌های فناوری است (بهره‌مند و عامری ثانی، ۱۳۹۸: ۶۲).

افزایش پیچیدگی در عملیات مادی پول‌شویی و سازمان‌یافتگی بیش‌ازپیش ارتکاب این بزه از یک سو و استفاده روزافزون از فناوری‌های نوین همچون «روش‌های نوین نقل‌وانتقال پول و سرمایه» از سوی دیگر، مقنن را بر آن داشت که با ایجاد نهادهای تخصصی نظارتی و کاشف نسبت به به‌روزرسانی فعالیت‌های پیشگیرانه اقدام نمایند. با وجود این گسترش ضابطان قضایی خاص نیز

در این مسیر همواره مورد توجه بوده است؛ ضرورتی که مبنای ایجاد نهادهایی همچون گروه ویژه اقدام مالی را فراهم آورد (قجاوند، ۱۳۹۹: ۴۸۴). در ایران نیز قانون مبارزه با پول‌شویی در ماده ۷، نهاد نظارتی «مرکز اطلاعات مالی» را پیش‌بینی نموده است. علاوه بر این فرایند توقیف و ضبط رمزارزها نیازمند تدوین مقررات جدیدی است که مشخص کند چگونه باید دارایی‌های دیجیتال غیرقانونی را مسدود، ضبط یا مصادره کرد. همچنین در قوانین سنتی، اموال فیزیکی یا حساب‌های بانکی به‌سادگی قابل توقیف هستند، اما در دنیای رمزارزها امکان انتقال سریع دارایی‌ها به کیف پول‌های غیرقابل ردیابی یا حتی صرافی‌های خارج از کشور وجود دارد که اجرای احکام را با چالش‌های جدی مواجه می‌کند. درنتیجه تدوین سازکارهای حقوقی مشخص برای مدیریت دارایی‌های دیجیتال مجرمانه و استفاده از فناوری‌های نظارتی پیشرفته، امری ضروری به نظر می‌رسد. یکی دیگر از چالش‌های کلیدی ناشی از ماهیت غیرمتمرکز ارزهای دیجیتال، موضوع «صلاحیت قضایی» است. تراکنش‌های ارزهای دیجیتال، می‌توانند در هر مکانی فراتر از مرزها رخ دهند که در حوزه‌های قضایی متعددی صلاحیت قضایی دارند (Ajayi & Udeh, 2024: 33). این موضوع می‌تواند باعث ایجاد ابهام در صلاحیت قضایی شود، زیرا مشخص نیست که قوانین کدام حوزه قضایی بر یک معامله و اقدام مالی خاص حاکم است. برای مثال اگر یک صرافی ارز دیجیتال در کشوری مستقر باشد، اما به کاربران چندین کشور خدمات ارائه دهد، تعیین اینکه قوانین کدام کشور بر فعالیت‌های آن صرافی اِعمال می‌شود، می‌تواند چالش‌برانگیز باشد. رسیدگی به این چالش‌های قضایی مستلزم همکاری و هماهنگی بین‌المللی میان نهادهای تنظیم‌کننده و سازمان‌های مجری قانون است (Uzougbo et al., 2024: 70).

۳-۲- توسعه و اجرای چهارچوب‌های نظارتی دیجیتال

امروزه با تحولاتی که در ارتکاب جرایم مالی از طریق فناوری‌های دیجیتال صورت گرفته، اصلاح نظام و ساختار نظارت و کنترل بر صرافی‌های رمزارزی و پلتفرم‌های مالی دیجیتال ضرورت دارد. در دوره کنونی، بسیاری از مبادلات رمزارزی در کشور ایران بدون نظارت قانونی انجام می‌شود و صرافی‌های داخلی به دلیل فقدان چهارچوب‌های نظارتی مشخص، الزام قانونی به احراز هویت مشتریان و رعایت مقررات مبارزه با پول‌شویی ندارند. گروه ویژه اقدام مالی، در سال ۲۰۱۹ اقدام به انتشار دستورالعمل‌های مقدماتی درخصوص ارزهای رمزنگاری‌شده کرد که طی آن ارائه‌دهندگان دارایی دیجیتال موظف به کسب مجوز یا ثبت‌نام در مراکز قانونی که این گروه به وجود آورده بود، شدند. همچنین صاحبان این مراکز قانونی موظف به ارائه اطلاعات هویتی مزبور به مقامات مربوطه شدند (مددی و قماشی، ۱۴۰۰: ۵۱۵).

به‌کارگیری تجزیه‌وتحلیل داده‌ها در راهبردهای مبارزه با پول‌شویی، تحول چشمگیری در

شیوه شناسایی، پیشگیری و مقابله با فعالیت‌های مالی غیرقانونی توسط بانک‌ها و مؤسسات مالی ایجاد کرده است. با پیچیده‌تر شدن تاکتیک‌های مجرمانه در پول‌شویی، سیستم‌های سنتی مبتنی بر قوانین، دیگر توانایی کافی برای مقابله با این تهدیدات در حال تحول را ندارند. ادغام تجزیه‌وتحلیل داده‌های پیشرفته، به‌ویژه نظارت لحظه‌ای[۱۳]، یادگیری ماشینی[۱۴] و اتوماسیون، راهکارهای نوآورانه‌ای ارائه می‌دهد که ضمن افزایش اثربخشی اقدامات مبارزه با پول‌شویی[۱۵]، تطابق با مقررات را نیز بهبود می‌بخشد.

نظارت دیجیتال بر تراکنش‌های رمزارزی از طریق فناوری‌های نوین به بانک‌ها و صرافی‌های رمزارزی، این امکان را می‌دهد که با سرعت و دقت بیشتری فعالیت‌های مشکوک را شناسایی کرده، موارد مثبت کاذب[۱۶] را کاهش دهند و از انطباق با مقررات در حال تغییر اطمینان حاصل کنند. در جهانی که تراکنش‌های مالی دیجیتال به‌سرعت انجام می‌شوند، توانایی پردازش و تحلیل داده‌ها در لحظه برای شناسایی فعالیت‌های مشکوک پیش از ایجاد زیان، امری حیاتی است. پردازش بلادرنگ داده‌ها به مؤسسات مالی و پلتفرم‌های تبادل رمزارزها، این امکان را می‌دهد که تراکنش‌های مشکوک را در همان لحظه شناسایی و بررسی کنند (به‌جای آنکه به بررسی‌های پس از وقوع متکی باشند) که اغلب منجر به از دست رفتن فرصت‌های پیشگیری از پول‌شویی می‌شود (Afeku-Amenyo, 2024; Scott et al., 2024: 868). نظارت لحظه‌ای در حوزه رمزارزها به صرافی‌ها و پلتفرم‌های مالی این امکان را می‌دهد که به‌سرعت الگوهای غیرعادی مانند «نقل‌وانتقالات ناگهانی، تبدیل‌های مکرر بین رمزارزهای مختلف و فعالیت‌های مرتبط با کیف پول‌های مشکوک» را شناسایی کنند. این قابلیت نقش حیاتی در جلوگیری از سوءاستفاده پول‌شویان از تأخیرهای موجود در سیستم‌های سنتی مبارزه با پول‌شویی دارد و مانع از انتقال وجوه غیرقانونی از طریق بلاکچین بدون شناسایی می‌شود.

هوش مصنوعی و یادگیری ماشینی، نقش اساسی در بهبود توانایی سیستم‌های بلادرنگ برای شناسایی ناهنجاری‌ها ایفا می‌کنند. این فناوری‌ها با تحلیل حجم گسترده‌ای از داده‌های تراکنشی در بلاکچین، الگوها و رفتارهایی را که ممکن است نشان‌دهنده پول‌شویی باشند، شناسایی می‌کنند. برخلاف سیستم‌های سنتی مبتنی بر قوانین که نیازمند تعریف آستانه‌ها و معیارهای از پیش تعیین‌شده هستند، مدل‌های هوش مصنوعی و یادگیری ماشین از داده‌های تاریخی می‌آموزند و به‌مرور زمان بهبود می‌یابند. این مدل‌ها قادرند انحرافات جزئی از الگوهای عادی را شناسایی کنند؛ مواردی که ممکن است در سیستم‌های مبتنی بر قوانین باعث هشدار

13. Real-time Monitoring
14. Machine Learning (ML)
15. Anti-Money Laundering (AML)
16. False Positives

نشوند، اما همچنان نشانه‌ای از فعالیت‌های مشکوک باشند. به‌عنوان مثال یک سیستم مجهز به هوش مصنوعی می‌تواند افزایش غیرمعمول تراکنش‌ها را در بازه‌های زمانی خاص تشخیص دهد یا ارتباطات میان کیف پول‌های درظاهر نامرتبط را شناسایی کند که ممکن است نشان‌دهنده عملیات لایه‌بندی برای پنهان‌سازی منشأ پول‌های غیرقانونی باشد. این انعطاف‌پذیری و هوشمندی، باعث می‌شود که سیستم‌های نظارت بلادرنگ مبتنی بر هوش مصنوعی در حوزه رمزارزها بسیار مؤثرتر از روش‌های سنتی عمل کرده و الگوهای پول‌شویی را که ممکن است از دید پنهان بمانند، شناسایی کنند (Eghaghe et al., 2024: 1897).

راهبرد تحولی دیگر در مبارزه با پول‌شویی دیجیتال، استفاده از «تحلیل‌های پیش‌بینی برای ارزیابی ریسک تراکنش‌های رمزارزی» است. تحلیل‌های پیش‌بینی، به مؤسسات مالی و پلتفرم‌های تبادل رمزارز این امکان را می‌دهد که احتمال وقوع پول‌شویی را با تحلیل داده‌های تاریخی و شناسایی الگوهایی که نشان‌دهنده ریسک احتمالی هستند، ارزیابی کنند. این فرایند شامل استفاده از الگوریتم‌های یادگیری ماشین است که بر روی داده‌های بلاکچینی گسترده تراکنش‌های گذشته، ازجمله موارد شناخته‌شده پول‌شویی، آموزش داده شده‌اند (Efunniyi, et al, 2024: 460). با شناسایی الگوها و ویژگی‌هایی که معمولاً با فعالیت‌های غیرقانونی مرتبط هستند، این مدل‌ها قادرند پیش‌بینی کنند که کدام تراکنش‌ها یا کیف پول‌ها در معرض ریسک بالاتری برای درگیر شدن در پول‌شویی قرار دارند.

مزیت اصلی تحلیل‌های پیش‌بینی در حوزه رمزارزها، توانایی آنها در فراتر رفتن از اقدامات واکنشی و امکان مداخله‌های پیشگیرانه است. به‌جای منتظر ماندن برای وقوع تراکنش‌های مشکوک، صرافی‌ها و نهادهای نظارتی می‌توانند از مدل‌های پیش‌بینی برای شناسایی کیف پول‌های پرریسک یا تراکنش‌های مشکوک قبل از وقوع هرگونه فعالیت غیرقانونی استفاده کنند و بدین ترتیب از وقوع پول‌شویی از ابتدا جلوگیری کنند. مثال‌های موفق در دنیای واقعی، کارایی تحلیل‌های پیش‌بینی‌کننده در مبارزه با پول‌شویی رمزارزی را نشان می‌دهند. یک پلتفرم بزرگ تبادل رمزارز با تجزیه‌وتحلیل داده‌های تراکنش‌های تاریخی در بلاکچین، موفق شد الگوهای رفتاری مشکوکی را شناسایی کند که پیش‌تر ناشناخته بودند (Eghaghe et al., 2024: 1898)؛ بنابراین لازم است که نهادهای ذی‌ربط مانند مرکز اطلاعات مالی، پلیس فتا و بانک مرکزی به ابزارهای پیشرفته تحلیل بلاکچین مجهز شوند. همچنین تصویب قوانینی برای الزام صرافی‌های رمزارزی به گزارش‌دهی تراکنش‌های مشکوک و ارائه اطلاعات کاربران به نهادهای نظارتی می‌تواند نقش مهمی در پیشگیری از پول‌شویی داشته باشد.

۳-۳- همکاری‌های بین‌المللی و همسوسازی نهادهای مالی و نظارتی

تحقیقات و تعقیب جرایم مالی دیجیتال که اغلب شامل بازیگران و قربانیانی در حوزه‌های قضایی

متعدد می‌شود، با پیچیدگی‌های مربوط به «صلاحیت قضایی دولت‌ها» مواجه است. ماهیت فرامرزی اینترنت و نظام‌های مالی دیجیتال، اِعمال چهارچوب‌های قانونی سنتی مبتنی بر قلمروی سرزمینی را دشوار می‌سازد و نیازمند تقویت همکاری‌های بین‌المللی است. به عبارتی همکاری‌های بین‌المللی از طریق کنوانسیون‌هایی همچون «کنوانسیون پالرمو[۱۷] و کنوانسیون بوداپست[۱۸]»، نقش حیاتی در «تسهیل استرداد مجرمین»، «معاضدت قضایی متقابل» و «تبادل اطلاعات در پرونده‌های جرایم مالی نوین» دارد. وقوع خسارت‌های فراگیر ناشی از بزه پول‌شویی در سرتاسر جهان، موجب تدوین اسناد بین‌المللی قابل‌توجهی با هدف مبارزه با پول‌شویی و جرایم سازمان‌یافته و تأمین مالی تروریسم شده که به‌تدریج موجب انتقال مقررات تدوینی به نظام‌های حقوقی داخلی بسیاری گشته است. کنوانسیون سازمان ملل متحد برای مبارزه با قاچاق مواد مخدر و داروهای روان‌گردان ۱۹۸۸ وین[۱۹]، کنوانسیون سازمان ملل متحد برای مبارزه با جرایم سازمان‌یافته فراملی ۲۰۰۰[۲۰]، کنوانسیون مبارزه با تأمین مالی تروریسم ۱۹۹۹[۲۱]، کنوانسیون سازمان ملل متحد برای مبارزه با فساد ۲۰۰۳ مریدا[۲۲] و توصیه‌های چهل‌گانه گروه ویژه اقدام مالی[۲۳] را می‌توان از مهم‌ترین اسناد بین‌المللی موجود در این خصوص به شمار آورد.

سازمان‌های بین‌المللی (مانند گروه ویژه اقدام مالی)، نقش کلیدی در مبارزه جهانی با پول‌شویی، به‌ویژه در حوزه رمزارزها ایفا می‌کنند و بر لزوم اجرای راهبردهای کارآمد مبارزه با پول‌شویی تأکید دارند که خود شامل «ایجاد استانداردهای جهانی، تسهیل تبادل اطلاعات درباره تکنیک‌های وقوع پول‌شویی و تأمین مالی تروریسم و نظارت بر رعایت مقررات توسط کشورهای عضو» است. در زمینه رمزارزها، این سازمان‌ها چهارچوب‌هایی را برای افزایش شفافیت تراکنش‌های دیجیتال و کاهش سوءاستفاده‌های مجرمانه تدوین کرده‌اند (Yusoff et al., 2024: 3). به‌عنوان مثال در سال ۲۰۱۸ گروه ویژه اقدام مالی، استانداردهای خود را درباره ارزهای دیجیتال و شرکت‌های مرتبط به‌روزرسانی کرد و دامنه مقررات مبارزه با پول‌شویی و تأمین مالی تروریسم را گسترش داد. طبق این دستورالعمل، ارائه‌دهندگان خدمات ارزهای دیجیتال باید تحت نظارت قوانین مذکور قرار گیرند. رعایت این مقررات علاوه بر کاهش جرایم مالی، از منافع مؤسسات مالی نیز محافظت می‌کند. همچنین این سازمان، با انتشار فهرست سیاه

17. Palermo Convention
18. Budapest Convention
19. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 1988.
20. United Nations Convention against Transnational Organized Crime, 2000.
21. International Convention for the Suppression of the Financing of Terrorism, 1999.
22. United Nations Convention against Corruption, Mérida, 2003.
23. Forty Recommendations of the Financial Action Task Force (FATF)

کشورهایی که این الزامات را رعایت نمی‌کنند، فشار بین‌المللی برای اجرای این مقررات را افزایش داده است (مددی و قماشی، ۱۴۰۰: ۵۱۵).

۳-۴- راهبردهای پیشگیرانه و بهره‌برداری از فناوری‌های نوین

بهبود سیاست‌های مبارزه با پول‌شویی، آموزش ساختاریافته کارکنان، تجزیه‌وتحلیل داده‌ها، گزارش‌دهی تراکنش‌های مشکوک و احراز هویت دقیق مشتریان، ازجمله اقدامات اساسی برای تقویت راهبردهای کاهش پول‌شویی هستند. اولین راهبرد، بهبود سیاست‌های مبارزه با پول‌شویی است (Unger, 2020).

در این راستا استفاده از رویکردهای نوین نظارتی و تقنینی می‌تواند نقش مؤثری در شناسایی و کاهش جرایم مالی ایفا کند. ازجمله اقدامات ضروری می‌توان به «تدوین فهرست مناطق پرخطر برای انجام تراکنش‌های مالی مشکوک»، «نظارت دقیق بر شرکت‌های صوری و حساب‌های فاقد هویت مشخص» و درنتیجه «ارتقای هماهنگی میان نهادهای نظارتی (مانند مرکز اطلاعات مالی و مبارزه با پول‌شویی، بانک مرکزی و سایر مراجع ذی‌صلاح)» اشاره کرد. این اصلاحات می‌تواند به انسجام بیشتر چهارچوب‌های قانونی و افزایش کارآمدی نظام مبارزه با پول‌شویی در ایران منجر شود.

دومین راهبرد اساسی در مقابله با پول‌شویی، «آموزش ساختاریافته کارکنان در نهادهای مالی و اقتصادی است. هر سازمان باید یک برنامه آموزشی جامع و رسمی برای آگاهی‌بخشی به کارکنان خود درباره سیاست‌های داخلی و بین‌المللی مبارزه با پول‌شویی تدوین کند. این آموزش‌ها باید شامل دستورالعمل‌های مشخصی درباره نحوه شناسایی تراکنش‌های مشکوک و اقداماتی باشد که کارکنان باید در مواجهه با سناریوهای مرتبط با پول‌شویی انجام دهند. به همین دلیل در نظام حقوقی ایران لازم است بانک‌ها، مؤسسات مالی، صرافی‌ها و سایر نهادهای مرتبط، تحت نظارت مرکز اطلاعات مالی و مبارزه با پول‌شویی، برنامه‌های آموزشی مستمری برای کارکنان خود برگزار کنند. به‌علاوه اجرای دوره‌های آموزشی الزامی و آزمون‌های ارزیابی برای کارکنان کلیدی این بخش‌ها می‌تواند به افزایش آگاهی و توانمندی آنها در شناسایی و گزارش‌دهی جرایم مالی کمک کند. همچنین تدوین مقرراتی برای الزام سازمان‌ها به ارائه گزارش‌های دوره‌ای درباره وضعیت آموزش کارکنان، می‌تواند موجب انسجام و اثربخشی بیشتر این سیاست‌ها شود. با این حال یکی از موانع اجرای مؤثر این سیاست‌ها، ترس کارکنان از اقدامات تلافی‌جویانه پس از گزارش‌دهی تخلفات است. بر اساس نظرسنجی جهانی اخلاق کسب‌وکار در سال ۲۰۲۰، ۶۱ درصد از کارمندان در سراسر جهان پس از گزارش سوءرفتار در سازمان‌های خود اعم از دولتی، خصوصی یا غیرانتفاعی با اقدامات تلافی‌جویانه مواجه شده‌اند

(Yusoff et al., 2024: 4).

بر اساس گزارش «گلوبال ایوای[۲۴]»، تحلیل داده‌ها (مانند هوش مصنوعی، پردازش زبان طبیعی و یادگیری ماشینی) می‌تواند به کاهش پول‌شویی کمک کند. این روش‌های پیشرفته تحلیل داده‌ها، ممکن است «فرایند شناسایی مشتری[۲۵]» را بهبود بخشند؛ مجوزهای مربوط به ارزیابی عملکرد را ارتقا دهند و درنهایت فعالیت‌های تراکنشی را نظارت کنند؛ که همین امر می‌تواند در شناسایی مؤثر ریسک‌ها و فرصت‌های مرتبط با پول‌شویی مفید باشد (Ujoodha & Suppiah, 2023: 3). هوش مصنوعی با بهره‌گیری از پایش لحظه‌ای تراکنش‌ها، تشخیص ناهنجاری‌ها و تحلیل پیش‌بینی‌کننده، نقش مؤثری در مقابله با چالش‌های امنیتی ایفا می‌کند. سیستم‌های ضد پول‌شویی مبتنی بر هوش مصنوعی از یادگیری ماشینی، پردازش زبان طبیعی و اتوماسیون فرایندهای رباتیک بهره می‌برند تا دقت شناسایی تقلب را افزایش داده، هزینه‌های عملیاتی را کاهش داده و استانداردهای نظارتی را رعایت کنند. بر اساس نتایج پژوهش‌های انجام‌شده، به‌کارگیری هوش مصنوعی در مبارزه با پول‌شویی منجر به کاهش ۷۰ درصدی فعالیت‌های مثبت‌های کاذب و افزایش ۳۰ درصدی در شناسایی رویدادهای پرریسک شده است (Gelle, 2025: 2462; Boateng et al., 2025: 37; Raj et al., 2024). با این حال چالش‌هایی نظیر «ضعف یکپارچگی داده‌ها، هزینه‌های بالا، ابهام در مقررات و ملاحظات اخلاقی»، ازجمله موانع اجرای این فناوری در سیستم‌های مالی محسوب می‌شوند.

با توجه به قوانین مرتبط، ازجمله «قانون مبارزه با پول‌شویی و آیین‌نامه‌های اجرایی مربوطه»، بهره‌گیری از این فناوری‌ها می‌تواند فرایند شناسایی مشتری را در بانک‌ها و مؤسسات مالی بهبود بخشد و از جعل هویت و تخلفات مالی جلوگیری کند. با این حال اجرای موفق این راهکارها در کشور ایران مستلزم «به‌روزرسانی زیرساخت‌های فناوری اطلاعات»، «تدوین قوانین حمایتی» و «ارتقای شفافیت در سیستم مالی» کشور است. هماهنگی میان بانک مرکزی، واحد اطلاعات مالی، شبکه بانکی و سایر نهادهای نظارتی نیز در این زمینه اهمیت ویژه‌ای دارد. راهبرد بعدی برای کاهش پول‌شویی، بررسی دقیق مشتری[۲۶] است. در این فرایند، چرخه زندگی مشتری به‌طور کامل مورد تحلیل قرار می‌گیرد؛ از سوابق اولیه تا تغییرات اساسی در طول زمان، همراه با بازبینی‌های منظم. برای شرکت‌ها ضروری است که شناخت عمیقی از مشتریان خود داشته باشند تا از سوءاستفاده پول‌شویان جلوگیری کرده و ریسک‌های احتمالی را به حداقل برسانند.

24. EY Global
25. Know Your Customer (KYC)
26. Customer Due Diligence (CDD)

نتیجه‌گیری و پیشنهادها

این پژوهش با هدف بررسی چالش‌های ناشی از سوءاستفاده از فناوری‌های نوین مالی در ارتکاب جرایم پول‌شویی و کلاهبرداری و ارائه راهکارهای مقابله‌ای مؤثر به انجام رسید. سؤال اصلی تحقیق بر این محور استوار بود که «چگونه می‌توان از طریق راهکارهای تقنینی، نظارتی و فناورانه، با این تهدیدات نوین به‌طور کارآمد مقابله کرد». یافته‌های تحقیق، فرضیات مطرح‌شده را تا حد زیادی تأیید می‌کند و نشان می‌دهد که ورود فناوری‌های مالی نوین، اگرچه منافع اقتصادی و اجتماعی فراوانی به همراه داشته، اما چشم‌انداز جرایم مالی را به‌طور اساسی دگرگون کرده است.

در پاسخ به فرضیه اول، پژوهش نشان داد که ویژگی‌های ذاتی فناوری‌هایی چون رمزارزها (مانند ناشناسی نسبی، تمرکززدایی، قابلیت انتقال فرامرزی سریع) و پیچیدگی ابزارهای دیجیتال، به‌طور قابل توجهی روش‌های سنتی پول‌شویی و کلاهبرداری را متحول ساخته و امکان پنهان‌سازی هویت مجرمان و منشأ وجوه غیرقانونی را از طریق تکنیک‌هایی مانند «مخلوط‌سازی تراکنش‌ها، استفاده از صرافی‌های غیرمجاز و بهره‌گیری از شبکه‌های تاریک» افزایش داده است. این امر، کارایی سازکارهای نظارتی و کشف جرم سنتی را به چالش کشیده و ضرورت بازنگری در رویکردهای مقابله‌ای را آشکار می‌سازد.

یافته‌های تحقیق در راستای تأیید فرضیه دوم، مؤید آن است که مقابله کارآمد با این پدیده نیازمند اتخاذ یک رویکرد جامع و چندوجهی است. صرف تکیه بر ابزارهای سنتی یا راهکارهای تک‌بعدی کافی نیست. این رویکرد باید شامل موارد زیر باشد:

۱- اصلاحات تقنینی و به‌روزرسانی مقررات قوانین کیفری و مالی باید به‌طور پویا با تحولات فناورانه همگام شوند. این امر مستلزم تعریف دقیق حقوقی دارایی‌های دیجیتال، جرم‌انگاری صریح سوءاستفاده از آنها در فعالیت‌های مجرمانه، تعیین مسئولیت برای ارائه‌دهندگان خدمات مالی دیجیتال و ایجاد رویه‌های قضایی مشخص برای توقیف و مدیریت دارایی‌های مجازی است. همان‌طور که بحث شد، خلأهای قانونی موجود، هم زمینه سوءاستفاده مجرمان را فراهم کرده و هم احقاق حق بزه‌دیدگان را با دشواری مواجه می‌سازد.

۲- توسعه چهارچوب‌های نظارتی دیجیتال. نهادهای ناظر مالی نیازمند توسعه و پیاده‌سازی چهارچوب‌های نظارتی هوشمند و مبتنی بر فناوری هستند. این چهارچوب‌ها باید بر شناسایی دقیق مشتری و اجرای مؤثر مقررات مبارزه با پول‌شویی و تأمین مالی تروریسم در فضای دیجیتال، به‌ویژه برای صرافی‌ها و

پلتفرم‌های رمزارزی تمرکز کنند. نظارت لحظه‌ای و تحلیل پیش‌بینی‌کننده داده‌ها در این زمینه نقشی کلیدی ایفا می‌کند.

۳- تقویت همکاری‌های بین‌المللی. با توجه به ماهیت فرامرزی جرایم مالی دیجیتال، همکاری مؤثر میان کشورها امری حیاتی است. تبادل اطلاعات، معاضدت قضایی، استرداد مجرمین و همسوسازی استانداردها (مانند استانداردهای FATF) برای مقابله با شبکه‌های جرایم سازمان‌یافته‌ای که از این فناوری‌ها بهره می‌برند، ضروری است. چالش‌های پیش روی ایران در این زمینه به دلیل عدم الحاق به برخی کنوانسیون‌ها و قرارگیری در فهرست‌های خاص، لزوم توجه ویژه به دیپلماسی حقوقی و فنی را دوچندان می‌کند.

در ارتباط با فرضیه سوم، پژوهش حاضر نشان داد که خودِ فناوری‌های نوین می‌توانند بخش مهمی از راه‌حل باشند. استفاده هوشمندانه از ابزارهایی مانند «هوش مصنوعی و یادگیری ماشینی» برای تحلیل الگوهای پیچیده تراکنش‌ها و شناسایی رفتارهای مشکوک، به‌کارگیری فناوری دفتر کل توزیع‌شده (بلاکچین) برای افزایش شفافیت (در چهارچوب‌های مجاز و کنترل‌شده) و تقویت ابزارهای امنیت سایبری پیشرفته، می‌تواند توانایی نهادهای مالی و انتظامی را در پیشگیری، کشف و واکنش به جرایم مالی نوین به میزان قابل توجهی ارتقا دهد. این رویکرد فناورانه باید مکمل روش‌های سنتی باشد و نه جایگزین آنها.

بنابراین در پاسخ نهایی به سؤال اصلی پژوهش، می‌توان گفت که مقابله مؤثر با پول‌شویی و کلاهبرداری‌های نوین از طریق فناوری‌های مالی، مستلزم یک راهبرد یکپارچه و پویا است که ترکیبی از قوانین و مقررات به‌روز و منعطف، نظارت دیجیتال هوشمند و مبتنی بر ریسک و بهره‌برداری راهبردی از فناوری‌های پیشرفته برای کشف و پیشگیری و همکاری فعال بین‌المللی باشد. علاوه بر این آموزش مستمر کارکنان نهادهای مالی و انتظامی و ارتقای آگاهی عمومی نسبت به مخاطرات، نقش مکمل و مهمی در کاهش آسیب‌پذیری‌ها ایفا می‌کند.

این تحقیق ضمن تبیین ابعاد مختلف چالش‌ها و راهکارها، بر لزوم اقدام سریع و هماهنگ میان سیاست‌گذاران، نهادهای نظارتی، بخش خصوصی و جامعه بین‌المللی تأکید می‌ورزد. تعلل در این زمینه می‌تواند منجر به گسترش آسیب‌های اقتصادی و تضعیف اعتماد به سیستم‌های مالی در عصر دیجیتال گردد. پژوهش‌های آتی می‌توانند بر ارزیابی اثربخشی مدل‌های خاص هوش مصنوعی در کشف پول‌شویی رمزارزی، تحلیل تطبیقی چهارچوب‌های نظارتی کشورهای پیشرو و بررسی راهکارهای عملیاتی برای غلبه بر موانع همکاری‌های بین‌المللی متمرکز شوند.

فهرست منابع

الف) منابع فارسی

- انصاری، جلال و علیرضا میلانی. (۱۳۹۵). نقد سیاست جنایی ایران در قبال کلاهبرداری اینترنتی. نشریه حقوق جزا و سیاست جنایی، ۱(۱).

- باصری، علی‌اکبر. (۱۳۸۷). سیاست جنایی قضایی کودکان و نوجوانان (در حقوق داخلی و اسناد بین‌المللی). تهران: انتشارات خرسندی.

- بهره‌مند، حمید و امیرکیا عامری ثانی. (۱۳۹۸). چالش‌ها و راهکارهای جرم‌یابی پول‌شویی از طریق ارزهای رمزنگاری‌شده. فصلنامه کارآگاه، ۱۳(۴۶).

- خرم‌آبادی، عبدالصمد. (۱۳۸۶). کلاهبرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران. فصلنامه حقوق مجله دانشکده حقوق و علوم سیاسی دانشگاه تهران، ۳۷ (۲).

- دهقان‌پور، امیرحسین. (۱۴۰۲). سیاست‌گذاری نسبت به اصل شفافیت اطلاعاتی در راستای پیشگیری از جرایم بازار اوراق بهادار. شانزدهمین کنفرانس بین‌المللی حقوق و علوم قضایی، لهستان.

- دیندار فرکوش، فیروز و حسین صدرنیا. (۱۳۸۸). روابط عمومی و رسانه. تهران: انتشارات سایه روشن.

- عزیزی، فاطمه و هادی سلیمانی. (۱۳۹۸). معرفی بیت‌کوین و چالش‌های امنیتی آن. نشریه علمی پدافند غیرعامل، ۱۰(۴).

- فراتی، مریم، باقر شاملو و ایرج گلدوزیان. (۱۳۹۹). راهکارهای مقابله با پول‌شویی از طریق بیت‌کوین. نشریه تحقیقات حقوقی بین‌المللی، ۱۳(۵۰).

- قجاوند، محسن. (۱۳۹۹). تحلیل تحولات نوین مبارزه با پول‌شویی در سیاست کیفری ایران. فصلنامه مطالعات حقوق کیفری و جرم‌شناسی، ۵۰(۲).

- لازرژ، کریستین. (۱۳۹۰). درآمدی بر سیاست جنایی. ترجمه: علی‌حسین نجفی ابرندآبادی. تهران: انتشارات میزان.

- مددی، مهدی و سعید قماشی. (۱۴۰۰). جستاری در پول‌شویی از طریق ارزهای رمزنگاری‌شده. فصلنامه مطالعات حقوق کیفری و جرم‌شناسی، ۵۱(۲).

- مغنی، حیدر، حمید ناصحی‌فر و تهمینه ناطق. (۱۳۹۸). چگونگی تأثیر گسترش فناوری‌های مالی بر بهبود عملکرد خدمات مالی. فصلنامه اقتصاد مالی، ۱۳(۴۹).

ب) منابع خارجی

- Afeku-Amenyo, Hilda. (2024). Employee sustainability knowledge: A catalyst for green finance product innovation. Business and Financial Times. Retrieved from https://thebftonline.com/2024/08/06/employee-sustainability-knowledge-a-catalyst.

- Ajayi, Funmilayo Aribidesi & Chioma Ann Udeh. (2024). Review of crew resilience and mental health practices in the marine industry: Pathways to improvement. *Magna Scientia Advanced Biology and Pharmacy*, 11(2). https://doi.org/10.30574/msabp.2024.11.2.0021

- Boateng, Victor, Elizabeth Kuukua Amoako, Ola Ajay & Tobias Kwame Adukpo. (2025). Harnessing Artificial Intelligence for combating money laundering and fraud in

the U.S. financial industry: A comprehensive analysis. *Finance & Accounting Research Journal*, 7(1). https://doi.org/10.51594/farj.v7i1.1814
- Castor, Amy. (2019). Spanish authorities: Bitcoin ATMs expose hole in AML laws. ATMmarketplace. Available at: https://www.atmmarketplace.com/articles/spanish-authorities-bitcoin-atms-expose-loophole-in-aml-laws/
- Efunniyi, Christianah Pelumi, Edith Ebele Agu, Abhulimen, Angela Omozele Abhulimen, & Anwuli Nkemchor Obiki-Osafiele. (2024). Sustainable banking in Africa: A review of Environmental, Social, and Governance (ESG) integration. *Finance & Accounting Research Journal*, 5(12). DOI:10.51594/farj.v5i12.1513
- Eghaghe, Vivian Ofure, Olajide Soji Osundare, Chikezie Paul-Mikki Ewim, Ifeanyi Chukwunonso Okeke. (2024). Advancing AML tactical approaches with data analytics: Transformative strategies for improving regulatory compliance in banks. *Finance & Accounting Research Journal* , 6(10). https://doi.org/10.51594/farj.v6i10.1644.
- Gelle, Venkata Raja Ravi Kumar. (2025). Enhancing financial security: AI-driven anti-money laundering (AML) and compliance monitoring in the banking sector. *World Journal of Advanced Research and Reviews*, 25(1). https://doi.org/10.30574/wjarr.2025.25.1.0365.
- Kartono, Kartono, Neva Sari Susanti, Samuel Soewita, Agus Salim & Ali Imron. (2024). Legal Ambiguity in Handling Cryptocurrency Evidence: Challenges and Solutions. *INJURITY: Journal of Interdisciplinary Studies*, 3(11). Available at: https://doi.org/10.58631/injurity.v3i11.1307
- Kepli, Mohd Yazid bin Zul & Sonny Zulhuda. (2019). Cryptocurrencies and Anti-money Laundering Laws: The Need for an Integrated Approach. In: *Emerging Issues in Islamic Finance Law and Practice in Malaysia.* pp. 247-263. Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-545-120191020
- Raj, Mayank., Khan, Hammad., Kathuria, Saksham., Chanti, Yash & Sahu, Mayank. (2024). *The Use of Artificial Intelligence in Anti-Money Laundering (AML)*. In: 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL) (pp. 272-277). IEEE. https://doi.org/10.1109/ICSADL61749.2024.00050
- Ruffing, Tim, Pedro Moreno-Sanchez & Aniket Kate. (2014). CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In: M. Kutyłowski & J. Vaidya (Eds.). *Computer Security – ESORICS 2014*. Lecture Notes in Computer Science, Vol. 8713, Springer, Cham. https://doi.org/10.1007/978-3-319-11212-1_20
- Savla, Sandeep. (2001). *Money Laundering and Financial Intermediaries* .London: Kluwer Law International.
- Scott, Anwulika, Prisca Amajuoyi & Kudirat Bukola Adeusi. (2024). Advanced risk management models for supply chain finance. *Finance & Accounting Research Journal*, 6(6). DOI:10.51594/farj.v6i6.1183
- Strehle, Elias & Lennart Ante. (2020) .Exclusive Mining of Blockchain Transactions. *BRL Working Paper Series*, (13). DOI:10.13140/RG.2.2.22494.05442
- Syahda, Illa Fatika, Rizki Dwi Putra, Tazkia Suhaila Syafa and Ester Stevany Putri Sinlae. (2024). Prevention and Eradication of Money Laundering Crime in Banking. *Veteran Law Review*, 7(2). DOI:10.35586/velrev.v7i2.8098
- Ujoodha, Yukta Shaivi and Kahyahthri Suppiah. (2023). Mitigating money laundering through technological and regulatory strategies. *E3S Web of Conferences*, 389. https://doi.org/10.1051/e3sconf/202338909031
- Unger, Brigitte. (2020). *Improving Anti-Money Laundering Policy .Policy Department for Economic, Scientific and Quality of Life Policies*. Luxembourg: European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648789/IPOL_STU(2020)6

48789_EN.pdf.
- Uzougbo, Ngozi Samuel, Chinonso Gladys Ikegwu & Adefolake Olachi Adewusi. (2024). International enforcement of cryptocurrency laws: Jurisdictional challenges and collaborative solutions. *Magna Scientia Advanced Research and Reviews* ,11(1). https://doi.org/10.30574/msarr.2024.11.1.0075.
- Yusoff, Yusri Hazrol, Syahirah Jumbli, Nur Nashuha Norazman, Nor Shahida Binti Abdul Razak & Muhamad Ridzuan Hashim. (2024). Enhancing Anti-Money Laundering Strategies: A Conceptual Paper. *Accounting and Finance Research*, 1(3). https://doi.org/10.5430/afr.v13n3p1.