

Copyright & Creative Commons:

The copyright of articles published in the *Journal of Financial and Economic Law Research* remains with the author(s). This journal is published as an open access publication, and all articles are distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0). This license permits use, redistribution, and reproduction in any medium, provided the original work is properly cited and the use is non-commercial in nature. For more information, please refer to the journal's *Open Access Policy* page.



Iran's Criminal Policy toward Monetary and Banking Crimes with an Emphasis on the Misuse of Financial Technologies: A Comparative Study with the European Union and the United States

Mahboubeh Ghorbani¹



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

Abstract

Monetary and banking crimes, together with the misuse of emerging financial technologies (FinTech), constitute significant challenges to contemporary financial and legal systems, posing serious threats to economic security and financial stability. The rapid expansion of financial technologies has facilitated the commission of offenses such as money laundering, cyber fraud, and the circumvention of regulatory and supervisory mechanisms, thereby compelling criminal justice systems to reconsider their legislative and enforcement policies. This study aims to examine Iran's criminal policy toward monetary and banking crimes, with particular emphasis on offenses arising from the misuse of financial technologies, through a comparative analysis of the legal frameworks of the European Union and the United States. Employing a descriptive-analytical methodology based on documentary and library research, the study compares Iranian laws and regulations, judicial practices, and institutional enforcement mechanisms with the legal standards and regulatory approaches adopted in the selected jurisdictions. The findings indicate that Iran's criminal policy in this field suffers from legislative gaps, inadequate supervision of financial institutions, limited alignment with international developments, and insufficient institutional coordination. By contrast, the European Union and the United States have adopted more effective approaches through preventive criminal policies, the deployment of advanced monitoring and tracking technologies, comprehensive

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

Article Type:
Original Research

DOI:
10.48300/jfel.2026.579872.1087

Received:
31 December 2025

Accepted:
1 March 2026

Published:
11 March 2026



1. M.A. in Private Law, West Tehran Branch, Islamic Azad University, Tehran, Iran.
Email: Mahboubehghorbani28@gmail.com

legislative frameworks, and robust enforcement mechanisms. The study concludes that enhancing the effectiveness of Iran's criminal policy requires comprehensive reform of criminal legislation, the development of digital supervisory infrastructure, the strengthening of regulatory institutions, the adoption of technology-oriented criminal policies, and greater harmonization with international legal standards governing technology-based financial crimes.

Keywords: Monetary and Banking Crimes; Criminal Policy; Financial Technologies (FinTech); European Union; United States.

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

Author contributions:

Mahboubeh Ghorbani: Conceptualization, Methodology, Software, Validation, Formal Analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization, Supervision, Project Administration.

Competing interests:

The authors declare that they have no competing interests.

Citation:

Ghorbani, Mahboubeh. (2025). Iran's Criminal Policy toward Monetary and Banking Crimes with an Emphasis on the Misuse of Financial Technologies: A Comparative Study with the European Union and the United States. *Journal of Financial and Economic Law*, 2(3): 337-379.

Extended Abstract

The rapid transformation of global financial systems through technological innovation has fundamentally altered the nature of financial transactions and the methods by which financial services are delivered. Financial technologies (FinTech), including digital payment systems, online banking platforms, cryptocurrencies, blockchain technology, artificial intelligence, and decentralized financial services, have significantly enhanced the efficiency, accessibility, and speed of financial operations. However, alongside these advantages, technological developments have also created new opportunities for criminal activities. The misuse of financial technologies has emerged as one of the most significant challenges confronting governments, financial institutions, regulatory authorities, and criminal justice systems worldwide. Crimes such as money laundering, cyber fraud, identity theft, unauthorized electronic transfers, terrorist financing, tax evasion, market manipulation, and cryptocurrency-related offenses have become increasingly sophisticated as a result of technological innovation and the cross-border nature of digital financial transactions. Financial and banking crimes not only cause substantial economic losses but also undermine public confidence in financial institutions, weaken national economic security, disrupt market stability, and threaten sustainable economic development. Consequently, governments have been compelled to redesign their criminal policies and legal frameworks to respond more effectively to these emerging forms of financial crime. Contemporary criminal policy extends beyond traditional punitive approaches and increasingly incorporates preventive strategies, regulatory oversight, technological monitoring, institutional coordination, and international cooperation. This study examines Iran's criminal policy toward financial and banking crimes, with particular emphasis on offenses committed through or facilitated by financial technologies. It also provides a comparative analysis of the Iranian legal framework alongside the criminal justice approaches adopted by the European Union and the United States. The purpose of this comparison is to identify the strengths and weaknesses of Iran's existing criminal policy, evaluate its effectiveness in combating technology-driven financial crimes, and propose practical legal and institutional reforms based on successful international experiences. The research adopts a descriptive-analytical methodology based on documentary and library research. National legislation, judicial decisions, executive regulations, policy documents, and academic literature relating to financial crimes are examined and analyzed. The study also reviews major international legal instruments, including anti-money laundering standards, counter-terrorist financing regulations, financial supervision mechanisms, and digital financial governance frameworks developed by the European Union and the United States. Through comparative legal analysis, similarities and differences among these legal systems are identified, enabling a comprehensive assessment of Iran's current legal framework. The findings demonstrate that, although Iran has enacted various laws and regulations to combat financial and banking crimes, its existing criminal policy continues to face significant legal, institutional, and technological challenges. One of the principal weaknesses is the absence of comprehensive legislation specifically designed to regulate emerging financial technologies and digital financial services. Existing legal provisions remain fragmented, largely reactive, and insufficiently adapted to rapidly evolving technological developments. Furthermore, supervisory institutions frequently suffer

from overlapping responsibilities, limited technological capacity, inadequate inter-agency coordination, and insufficient access to real-time financial monitoring systems. Another major challenge concerns the detection and prosecution of complex financial crimes involving cryptocurrencies, anonymous digital transactions, international financial networks, and cyber-enabled banking fraud. The absence of specialized investigative units, limited judicial expertise in handling digital financial evidence, and inadequate integration of advanced technological tools substantially reduce the effectiveness of criminal enforcement. Moreover, existing regulatory mechanisms often emphasize punitive measures after the commission of offenses rather than adopting preventive and risk-based approaches capable of identifying suspicious activities before significant financial harm occurs. In contrast, the European Union and the United States have developed more comprehensive criminal policies that integrate preventive regulation, technological innovation, institutional cooperation, and robust enforcement mechanisms. These jurisdictions have established sophisticated anti-money laundering systems, digital transaction monitoring platforms, mandatory customer due diligence procedures, beneficial ownership transparency requirements, financial intelligence units, cybersecurity regulations, and advanced risk assessment models. The use of artificial intelligence, big data analytics, blockchain forensic technologies, and international information-sharing mechanisms has substantially strengthened their capacity to detect, investigate, and prosecute complex financial crimes. The comparative analysis indicates that the effectiveness of criminal policy increasingly depends on integrating legal reforms with technological capabilities rather than relying solely on criminal sanctions. Modern strategies for preventing financial crime require dynamic legislation capable of adapting to technological innovation, highly trained investigators and judges, specialized prosecution offices, independent regulatory authorities, effective financial supervision, and sustained cooperation with international organizations engaged in combating financial crime. Based on these findings, the study recommends several policy reforms for Iran. These include revising criminal legislation to address emerging FinTech-related offenses, strengthening supervisory and regulatory institutions, expanding digital financial monitoring infrastructure, establishing specialized cyber-financial investigation units, enhancing judicial and prosecutorial expertise in digital evidence, promoting cooperation between financial institutions and law enforcement agencies, adopting risk-based regulatory approaches, improving transparency in financial transactions, and aligning domestic legislation with internationally recognized standards for combating financial crime and money laundering. Ultimately, the study concludes that the increasing complexity of financial technologies requires criminal policy to evolve from a predominantly punitive model toward a comprehensive, preventive, technology-oriented, and internationally coordinated framework. Such an approach would significantly enhance Iran's capacity to combat financial and banking crimes, protect economic security, reinforce public confidence in financial institutions, and strengthen the resilience of the national financial system in the face of rapidly evolving technological challenges.



سیاست‌های جنایی ایران در قبال بزه‌های پولی - بانکی با تأکید بر سوءاستفاده از فناوری‌های مالی: بررسی تطبیقی با اتحادیه اروپا و ایالات متحده آمریکا

محبوبه قربانی^۱

چکیده

بزه‌های پولی - بانکی و سوءاستفاده از فناوری‌های نوین مالی از جمله چالش‌های نوظهور در نظام‌های مالی و حقوقی محسوب می‌شوند که پیامدهای گسترده‌ای بر امنیت اقتصادی و ثبات مالی کشورها بر جای می‌گذارند. گسترش فناوری‌های مالی بستر ارتکاب جرایمی چون پول‌شویی، کلاهبرداری سایبری و دور زدن سازکارهای نظارتی را تسهیل کرده و نظام‌های کیفری را با ضرورت بازاندیشی در سیاست‌های تقنینی و اجرایی مواجه ساخته است. این پژوهش با هدف بررسی سیاست‌های جنایی ایران در قبال بزه‌های پولی - بانکی به‌ویژه در حوزه سوءاستفاده از فناوری‌های مالی، انجام شده و در چهارچوبی تطبیقی با نظام‌های حقوقی اتحادیه اروپا و ایالات متحده آمریکا به تحلیل نقاط قوت و ضعف سیاست‌های کیفری ایران پرداخته است. روش تحقیق توصیفی - تحلیلی و مبتنی بر مطالعات اسنادی و کتابخانه‌ای است و در آن قوانین و مقررات داخلی، رویه‌های قضایی و ساختارهای اجرایی ایران با تجارب و چهارچوب‌های حقوقی کشورهای مذکور مورد مقایسه قرار گرفته است. یافته‌ها نشان می‌دهد که سیاست جنایی ایران در این حوزه با خلأهای تقنینی، ضعف نظارتی بر نهادهای مالی، ناهماهنگی با تحولات بین‌المللی و نبود انسجام نهادی مواجه است. در مقابل، اتحادیه اروپا و آمریکا با اتخاذ رویکردهای پیشگیرانه، بهره‌گیری از فناوری‌های ردیابی هوشمند، تدوین قوانین جامع و اعمال ضمانت اجرای قوی توانسته‌اند



پژوهش‌های حقوق

نوع مقاله: علمی - پژوهشی

DOI:

10.48300/jel.2926.579872.1087

تاریخ دریافت:

۱۰ دی ۱۴۰۴

تاریخ پذیرش:

۱۰ اسفند ۱۴۰۴

تاریخ انتشار:

۲۰ اسفند ۱۴۰۴



۱. کارشناسی ارشد حقوق خصوصی، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران.

الگوهای موفق‌تری ارائه دهند. بر این اساس بازنگری در قوانین کیفری، ارتقای زیرساخت‌های نظارت دیجیتال، توانمندسازی نهادهای نظارتی، تدوین سیاست‌های جنایی فناورانه و هماهنگی با استانداردهای بین‌المللی از الزامات بهبود کارآمدی سیاست جنایی ایران در مواجهه با جرایم مالی مبتنی بر فناوری است.

کلیدواژه‌ها: بزه‌های پولی - بانکی، سیاست جنایی، فناوری‌های مالی، اتحادیه اروپا، ایالات متحده آمریکا.

حامی مالی:

این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:

محبوبه قربانی: مفهوم‌سازی، روش‌شناسی، استفاده از نرم‌افزار، اعتبارسنجی، تحلیل، تحقیق و بررسی، منابع، نظارت بر داده‌ها، نوشتن - پیش‌نویس اصلی، نوشتن - بررسی و ویرایش، تصویرسازی، نظارت، مدیریت پروژه.

تعارض منافع:

بنابر اظهار نویسندگان این مقاله تعارض منافع ندارد.

استناددهی:

قربانی، محبوبه. (۱۴۰۴). سیاست‌های جنایی ایران در قبال بزه‌های پولی - بانکی با تأکید بر سوءاستفاده از فناوری‌های مالی: بررسی تطبیقی با اتحادیه اروپا و ایالات متحده آمریکا. مجله پژوهشهای حقوق مالی و اقتصادی، ۲(۳)، ۳۳۷-۳۷۹.

مقدمه

در دهه‌های اخیر، پیشرفت فناوری‌های مالی^۲ تأثیرات شگرفی بر نظام‌های بانکی و مالی در سراسر جهان گذاشته است. این تحولات ضمن تسهیل دسترسی به خدمات مالی، چالش‌های نوینی را نیز در حوزه سیاست‌های جنایی و حقوق کیفری ایجاد کرده‌اند. یکی از مهم‌ترین این چالش‌ها بروز جرایم پولی - بانکی با استفاده از ابزارهای نوین مالی و فناوری‌های پیشرفته است که موجب پیچیدگی در شناسایی، پیشگیری و مقابله با این دسته از جرایم شده است. کشورهای مختلف به تناسب ساختارهای اقتصادی، حقوقی و قضایی خود سیاست‌های گوناگونی را برای مبارزه با این جرایم اتخاذ کرده‌اند که بررسی تطبیقی آنها می‌تواند به شناسایی نقاط ضعف و قوت نظام حقوقی ایران در این حوزه کمک کند.

تحولات سریع در حوزه فناوری‌های مالی در دهه‌های اخیر زمینه‌های جدیدی را برای ارائه خدمات مالی فراهم کرده است. این تحولات هرچند مزایای چشمگیری مانند تسهیل تراکنش‌های مالی، کاهش هزینه‌های بانکی و افزایش شفافیت در نظام مالی را به همراه داشته اما در عین حال بستر مناسبی را برای ارتکاب بزه‌های پولی - بانکی فراهم کرده است (Arner et al., 2016). ظهور پلتفرم‌های پرداخت آنلاین، رمزارزها، قراردادهای هوشمند و بانکداری دیجیتال راه‌های جدیدی را برای پول‌شویی، کلاهبرداری مالی، تأمین مالی تروریسم و سایر تخلفات بانکی ایجاد کرده است. در ایران نیز همانند بسیاری از کشورها، سیاست‌های جنایی برای مقابله با این نوع بزه‌ها در حال تحول است. با این حال چالش‌هایی مانند ضعف قوانین نظارتی، نبود هماهنگی بین نهادهای اجرایی و فقدان ابزارهای نظارت دیجیتال کارآمد، به گسترش سوءاستفاده از فناوری‌های مالی دامن زده است (مرکز پژوهش‌های مجلس، ۱۴۰۰). در حالی که اتحادیه اروپا و ایالات متحده آمریکا سازکارهای قانونی و اجرایی جامعی را برای کنترل و پیشگیری از این تخلفات توسعه داده‌اند، سیاست‌های جنایی ایران همچنان با کاستی‌های جدی مواجه است. این پژوهش با تمرکز بر سیاست‌های جنایی ایران در قبال بزه‌های پولی - بانکی، تلاش دارد تا ضمن بررسی قوانین و مقررات موجود، کاستی‌ها و چالش‌های اجرایی این سیاست‌ها را شناسایی کند. همچنین از طریق مطالعه تطبیقی با اتحادیه اروپا و ایالات متحده راهکارهای بهینه‌ای را برای بهبود سیاست‌های جنایی ایران ارائه خواهد داد.

باوجود پژوهش‌های متعدد در حوزه جرایم مالی، پول‌شویی، جرایم بانکی و آثار فناوری‌های مالی بر نظام‌های اقتصادی، تاکنون مطالعه‌ای جامع که به‌صورت هم‌زمان «سیاست جنایی ایران در قبال بزه‌های پولی - بانکی مبتنی بر فناوری‌های مالی» را در چهارچوبی تطبیقی با اتحادیه

اروپا و ایالات متحده آمریکا مورد تحلیل قرار دهد، کمتر مشاهده می‌شود. بخش عمده پژوهش‌های پیشین فقط بر ابعاد کیفری پول‌شویی، مسئولیت بانک‌ها یا مقررات مبارزه با جرایم سایبری متمرکز بوده‌اند و کمتر به پیوند میان سیاست جنایی، فناوری‌های مالی نوین و کارآمدی ساختارهای نظارتی پرداخته‌اند.

ازجمله مهم‌ترین پژوهش‌های مرتبط می‌توان به مطالعات آرner و همکاران (Arner et al., 2016) درخصوص چالش‌های حقوقی فناوری‌های مالی، پژوهش زتسه (Zetzsche et al., 2017) درباره تنظیم‌گری فین‌تک در اتحادیه اروپا و همچنین تحقیقات داخلی پیرامون قانون مبارزه با پول‌شویی و جرایم بانکی اشاره کرد. با این حال این آثار اغلب فاقد رویکرد تطبیقی جامع میان نظام حقوقی ایران و الگوهای پیشرفته بین‌المللی بوده و کمتر به ارزیابی سیاست جنایی اجرایی و قضایی در حوزه سوءاستفاده از فناوری‌های مالی پرداخته‌اند. نوآوری اصلی این پژوهش در چند محور قابل تبیین است:

۱. بررسی هم‌زمان سیاست جنایی تقنینی، قضایی و اجرایی ایران در حوزه بزه‌های پولی - بانکی مبتنی بر فناوری‌های مالی؛
۲. تحلیل تطبیقی ساختارهای حقوقی ایران با دو نظام پیشرو، یعنی اتحادیه اروپا و ایالات متحده آمریکا؛
۳. تمرکز بر نقش فناوری‌های نوین نظیر رمزارزها، بانکداری دیجیتال، قراردادهای هوشمند و سامانه‌های پرداخت الکترونیکی در تحول بزه‌های مالی؛
۴. ارائه راهکارهای سیاست‌گذاری مبتنی بر تنظیم‌گری هوشمند، نظارت دیجیتال و بهره‌گیری از فناوری‌های ردیابی مالی؛ و
۵. تحلیل چالش‌های نهادی و ضعف هماهنگی میان دستگاه‌های نظارتی و قضایی ایران در مقابله با جرایم مالی فناورانه.

پلان و ساختار مقاله بر مبنای یک منطق تحلیلی - تطبیقی تنظیم شده است؛ بدین‌صورت که ابتدا مبانی نظری و مفهومی بزه‌های پولی - بانکی و فناوری‌های مالی تبیین شده، سپس سیاست‌های جنایی ایران مورد بررسی قرار گرفته و در ادامه با مطالعه تطبیقی نظام‌های اتحادیه اروپا و ایالات متحده، نقاط قوت و ضعف سیاست جنایی ایران تحلیل شده است. درنهایت نیز با جمع‌بندی یافته‌ها، پیشنهادهایی جهت اصلاح ساختار تقنینی، نظارتی و اجرایی ایران ارائه شده است.

۱-۱- مبانی نظری

سیاست‌های جنایی در قبال جرایم پولی - بانکی به‌ویژه در حوزه سوءاستفاده از فناوری‌های مالی

بر پایه نظریه‌های مختلفی در حقوق کیفری و حقوق بانکی استوار است. یکی از مهم‌ترین مبانی نظری، نظریه پیشگیری از جرم^۳ است که بر اهمیت اقدامات نظارتی و کنترلی جهت کاهش فرصت‌های ارتکاب جرم تأکید دارد. این نظریه به‌ویژه در حوزه جرایم مالی از طریق ابزارهای نظارت بانکی، گزارش‌دهی الزامی و توسعه فناوری‌های کشف تقلب و پول‌شویی نمود می‌یابد. علاوه بر این نظریه واکنش اجتماعی^۴ نیز در تدوین سیاست‌های جنایی مالی نقش دارد. بر اساس این نظریه، نحوه تنظیم‌گری و میزان جرم‌انگاری و واکنش‌های کیفری یا غیرکیفری نسبت به تخلفات مالی می‌تواند بر رفتار فعالان اقتصادی تأثیرگذار باشد. سیاست‌های جنایی افتراقی که در برخی کشورها اعمال می‌شود، نشان می‌دهد که واکنش کیفری در همه موارد بهترین راه‌حل نیست و سازکارهای جایگزینی همچون ضمانت‌های اداری و انتظامی می‌تواند کارآمدتر باشد. در نظام‌های حقوقی پیشرفته، نظریه مقررات هوشمند^۵ نیز مورد توجه قرار گرفته است. این نظریه بر استفاده از ترکیبی از ابزارهای حقوقی، فنی و اقتصادی جهت کنترل جرایم مالی تأکید دارد. برای مثال در اتحادیه اروپا و ایالات متحده علاوه بر مجازات‌های کیفری، ابزارهایی همچون افشای الزامی تراکنش‌های مشکوک، محدودیت‌های معاملاتی و فناوری‌های شناسایی مشتری^۶ برای پیشگیری از سوءاستفاده‌های مالی به کار گرفته شده‌اند.

پژوهش‌های انجام‌شده در این حوزه چه در سطح داخلی و چه در سطح بین‌المللی نشان‌دهنده اهمیت روزافزون سیاست‌های جنایی در مواجهه با جرایم پولی - بانکی هستند. در ایران برخی پژوهش‌ها به بررسی چهارچوب‌های قانونی مبارزه با جرایم مالی و پول‌شویی پرداخته‌اند. برای مثال تحقیقات انجام‌شده در حوزه مقررات بانک مرکزی و قوانین مبارزه با پول‌شویی نشان داده است که ضعف در هماهنگی میان نهادهای نظارتی و نبود سازکارهای کنترلی مؤثر، زمینه سوءاستفاده از فناوری‌های مالی را فراهم کرده است. همچنین برخی پژوهش‌ها بر ناکارآمدی ضمانت‌های اجرایی موجود و نیاز به به‌روزرسانی قوانین متناسب با فناوری‌های مالی جدید تأکید داشته‌اند.

در سطح بین‌المللی مطالعاتی در اتحادیه اروپا و ایالات متحده آمریکا به تحلیل سیاست‌های کیفری و تنظیم‌گری مالی پرداخته‌اند. به‌عنوان مثال مطالعات انجام‌شده در اتحادیه اروپا نشان می‌دهد که «دستورالعمل چهارم و پنجم ضد پول‌شویی» اتحادیه اروپا تأثیر بسزایی در کاهش جرایم مالی داشته است. همچنین تحقیقات در ایالات متحده بر کارآمدی «قانون رازداری

3. Crime Prevention Theory

4. Social Reaction Theory

5. Smart Regulation

6. Know Your Customer (KYC)

بانکی^۷ و «قانون میهن پرستی»^۸ در شناسایی فعالیت‌های مشکوک تأکید دارند. در این کشورها استفاده از فناوری‌های نوین مانند هوش مصنوعی در تحلیل داده‌های مالی و پیشگیری از تقلب نیز به عنوان یک راهکار مؤثر، مورد بررسی قرار گرفته است.

هدف اصلی این پژوهش بررسی اثربخشی سیاست‌های جنایی ایران در مقابله با بزه‌های پولی - بانکی با تأکید بر سوءاستفاده از فناوری‌های مالی و مقایسه آن با سیاست‌های جنایی در اتحادیه اروپا و ایالات متحده است. این پژوهش همچنین در پی ارائه راهکارهایی برای ارتقای نظام نظارتی و کیفری ایران در این حوزه است. اهداف فرعی پژوهش عبارت‌اند از:

- بررسی نقاط قوت و ضعف قوانین ایران در زمینه جرایم مالی مرتبط با فناوری‌های نوین.
- تحلیل سیاست‌های جنایی اتحادیه اروپا و ایالات متحده در قبال این جرایم.
- مقایسه سیاست‌های تقنینی، قضایی و اجرایی ایران با نظام‌های حقوقی مذکور.
- ارائه پیشنهادهایی برای اصلاح قوانین و بهبود سیاست‌های پیشگیری و مقابله با این نوع جرایم.

بر این اساس، سؤالات اصلی پژوهش عبارت‌اند از:

۱. سیاست‌های جنایی ایران در قبال بزه‌های پولی - بانکی چه نقاط قوت و ضعفی دارد؟
۲. اتحادیه اروپا و ایالات متحده آمریکا چه رویکردهایی را برای مقابله با سوءاستفاده از فناوری‌های مالی اتخاذ کرده‌اند؟
۳. چگونه می‌توان سیاست‌های جنایی ایران را بر اساس الگوهای موفق بین‌المللی اصلاح و بهبود بخشید؟

بر این اساس فرضیه‌های پژوهش به شرح زیر تدوین شده‌اند:

- به نظر می‌رسد که سیاست‌های جنایی ایران در حوزه مقابله با جرایم پولی - بانکی به دلیل خلأهای قانونی و ضعف نظارت نسبت به استانداردهای بین‌المللی کارایی کمتری دارد.
- تجربه کشورهای پیشرو نشان می‌دهد که استفاده از ترکیبی از تدابیر کیفری، اداری و فناوری محور می‌تواند در مقابله با سوءاستفاده از فناوری‌های مالی اثربخش‌تر باشد.
- اصلاح قوانین ناظر بر جرایم پولی - بانکی، افزایش شفافیت در فرایندهای مالی و

7. Bank Secrecy Act (BSA)

8. Patriot Act

تقویت همکاری‌های بین‌المللی می‌تواند به بهبود سیاست‌های جنایی ایران در این حوزه کمک کند.

۱-۲- روش‌شناسی و رویکرد تطبیقی

این پژوهش از روش توصیفی - تحلیلی و تطبیقی بهره می‌برد. در بخش توصیفی، به بررسی قوانین و مقررات موجود در ایران پرداخته شده است. سپس در بخش تحلیلی، کاستی‌های این قوانین شناسایی شده و نقاط ضعف سیاست‌های جنایی ایران مورد ارزیابی قرار گرفته است. در بخش تطبیقی، سیاست‌های جنایی اتحادیه اروپا و ایالات متحده آمریکا مورد بررسی قرار گرفته و با نظام حقوقی ایران مقایسه شده است. برای گردآوری داده‌ها از روش کتابخانه‌ای استفاده شده و منابعی همچون قوانین و مقررات داخلی و بین‌المللی، گزارش‌های نهادهای نظارتی، مقالات علمی و کتب تخصصی در این حوزه مورد بررسی قرار گرفته‌اند. تحلیل داده‌ها نیز بر مبنای روش کیفی انجام شده است تا الگوهای سیاست‌گذاری و تفاوت‌های میان نظام‌های حقوقی شناسایی شود.

- رویکرد تطبیقی پژوهش بر مبنای تحلیل سیاست‌های کیفری در سه حوزه اصلی است:
- سیاست جنایی تقنینی: مقایسه قوانین کیفری و مقررات نظارتی ایران با اتحادیه اروپا و ایالات متحده.
- سیاست جنایی قضایی: بررسی رویه‌های قضایی مرتبط با بزه‌های پولی - بانکی در نظام‌های حقوقی مذکور.
- سیاست جنایی اجرایی: تحلیل سازکارهای نظارتی، فناوری‌های کنترلی و نقش نهادهای اجرایی در این سه نظام حقوقی.

این روش‌شناسی امکان شناسایی نقاط ضعف و قوت سیاست‌های جنایی ایران را فراهم می‌آورد و زمینه‌ساز ارائه پیشنهادهای عملی برای اصلاح و بهبود این سیاست‌ها خواهد شد. مطالعات داخلی و بین‌المللی حاکی از آن است که سیاست‌های جنایی مؤثر در حوزه جرایم پولی - بانکی، باید علاوه بر ابزارهای کیفری، بر سازکارهای پیشگیرانه، شفافیت مالی و تنظیم‌گری هوشمند تمرکز داشته باشند. در ایران، ضعف در اجرای مقررات، عدم هماهنگی میان نهادهای نظارتی و خلأهای قانونی از جمله موانع اساسی در مقابله با این جرایم هستند. بنابراین بهره‌گیری از تجربیات موفق کشورهای توسعه‌یافته و تطبیق آنها با مقتضیات نظام حقوقی ایران می‌تواند راهگشای اصلاح و بهبود سیاست‌های جنایی در این حوزه باشد. با توجه به افزایش روزافزون تخلفات مالی و بانکی که با استفاده از ابزارهای فناوری‌های نوین مالی صورت می‌گیرد، ضرورت دارد که نظام حقوقی ایران به‌روزرسانی شده و با تکیه بر تجربیات موفق سایر کشورها، اقدامات

مؤثرتری را در این زمینه اتخاذ کند. اهمیت این پژوهش در آن است که ضمن تحلیل انتقادی قوانین و مقررات فعلی، پیشنهادهایی عملی برای بهبود سیاست‌های کیفری و پیشگیرانه ارائه می‌دهد که می‌تواند مورد استفاده قانونگذاران، نهادهای نظارتی و دستگاه قضایی کشور قرار گیرد. درنهایت این پژوهش می‌تواند به غنی‌سازی ادبیات حقوقی در حوزه سیاست‌های جنایی مالی کمک کرده و به‌عنوان مرجع برای مطالعات آتی در این زمینه مورد استفاده قرار گیرد.

۲- چهارچوب نظری و مفهومی

در این بخش، مبانی نظری و مفهومی پژوهش با تمرکز بر تعریف بزه‌های پولی - بانکی، تبیین سوءاستفاده از فناوری‌های مالی، بررسی پیوند این فناوری‌ها با بزه‌های نوظهور اقتصادی و تحلیل پیامدهای آنها بر اقتصاد ملی و بین‌المللی مورد بررسی قرار می‌گیرد.

۲-۱- تعریف بزه‌های پولی - بانکی و ویژگی‌های آنها

بزه‌های پولی - بانکی به مجموعه‌ای از جرایم اطلاق می‌شود که در بستر نظام بانکی و مالی رخ داده و اغلب به دنبال نقض مقررات اقتصادی، سوءاستفاده از منابع مالی و دور زدن نظام‌های نظارتی و کنترلی هستند (Savona & Riccardi, 2017). این بزه‌ها شامل تخلفات متعددی از جمله پول‌شویی، کلاهبرداری مالی، اختلاس، تأمین مالی تروریسم، فرار مالیاتی و دست‌کاری در اطلاعات مالی می‌شوند (Levi, 2010).

از طرفی سیاست‌های اقتصادی دولت شامل سیاست‌های پولی، مالی و درآمدی می‌شود. سیاست‌های پولی به‌عنوان یکی از ابزارهای کلیدی برای تثبیت اقتصاد، نقش مهمی در مدیریت و کنترل بخش واقعی اقتصاد ایفا می‌کنند. این سیاست‌ها به‌عنوان یکی از روش‌های مؤثر برای افزایش تولید و اشتغال و همچنین بهره‌برداری از ظرفیت‌های بیکار جامعه به‌منظور توسعه و آبادانی کشور و رفع نگرانی‌های اقشار مختلف مردم به شمار می‌روند. سیاست پولی کشور توسط بانک مرکزی تعیین و اعلام می‌شود و این کار از طریق ابزارهایی نظیر حداقل ذخیره قانونی، تعیین نرخ بهره مجدد، عرضه اوراق مشارکت و غیره انجام می‌گیرد. بخشی از رفتارهای مجرمانه که مخالف این نوع سیاست‌ها بوده، به خلق مجرمانه پول مرتبط است که علاوه بر اخلاق در نظام پولی و بانکی و تورم، منفعت مادی برای مرتکب نیز به دنبال دارد. این نوع از رفتارهای مجرمانه از این جهت جرم علیه سیاست اقتصادی دولت در حوزه بانکی محسوب می‌شود که علاوه بر افزایش حجم پول و کاهش ارزش آن و سلب اعتماد عمومی در عمل کنترل و نظارت بانک مرکزی را که متولی ضرب سکه و چاپ اسکناس است، مختل می‌کند (میرمحمدصادقی، ۱۳۹۲: ۲۲۸). بخشی دیگر از جرایم بانکی، جرایمی هستند که به قصد تحصیل مجرمانه پول ارتکاب می‌یابند. جرایمی مانند جرایم بورسی، جرایم مربوط به قیمت‌ها، اوراق مشارکت، ربا و درنهایت قاچاق کالا

و ارز در این دسته قرار می‌گیرند (میرزایی منفرد، ۱۳۸۹؛ نورزاد، ۱۳۸۹: ۱۴۷).

بانک، نهادی اقتصادی است که وظیفه‌هایی چون تجهیز و توزیع اعتبارات، عملیات اعتباری، عملیات مالی، خرید و فروش ارز، نقل و انتقال وجوه، وصول مطالبات اسنادی و سود سهام مشتریان، پرداخت بدهی مشتریان، قبول امانات، نگهداری سهام و اوراق بهادار و اشیای قیمتی مشتریان، انجام وظیفه قیمومیت و وصایت برای مشتریان و انجام وکالت خرید یا فروش را بر عهده دارند (عزیزی، ۱۳۹۷: ۳۰-۳۱). بانک‌ها را می‌توان به دسته‌های مختلفی از جمله بانکداری جزئی، تجاری، مشارکتی، خصوصی و سرمایه‌گذاری تقسیم‌بندی کرد. در بانک‌های دولتی هر نوع جرم به وقوع پیوسته به‌طور قطع به‌عنوان جرم اقتصادی محسوب می‌شود، زیرا این جرایم هم دارای بستر اقتصادی هستند و هم تأثیراتی بر اقتصاد دارند. اما هر جرم اقتصادی همیشه به معنای جرم بانکی نیست. با ظهور بانک‌های خصوصی و مؤسسات مالی و اعتباری، این رابطه دچار تغییراتی شد و دامنه قوانین از بانک‌های دولتی فراتر رفت. در حال حاضر هر جرمی که در حوزه بانکداری اتفاق بیفتد، به‌عنوان جرم اقتصادی^۹ شناخته می‌شود و هر جرم اقتصادی نیز معادل جرم بانکی خواهد بود؛ به عبارت دیگر این دو رابطه‌ای عمومی و خاص دارند. از آنجایی که در اصطلاح جرایم بانکی واژه «بانک» به‌صورت عام و کلی به کار رفته است، بنابراین تمامی بانک‌ها و مؤسسات اعتباری و پولی که مجوز فعالیت آنها توسط بانک مرکزی صادر شده و تحت نظارت آن قرار دارند، در این تحقیق مورد بررسی قرار خواهند گرفت. زیرا هر نوع بانکی به‌نوعی با مفهوم پول در ارتباط است و مانند قلبی است که پول را در رگ‌های جامعه به جریان می‌اندازد؛ بنابراین هرگونه تغییر یا اختلال در عملکرد این قلب می‌تواند جامعه را دچار مشکلات جدی کند.

حال با مذاقه در مقررات ایران و اسناد بین‌المللی، هرچند اصطلاحی تحت عنوان «جرم بانکی» در متون قانونی به کار نرفته است، اما در مطالعات جرم‌شناختی مجموع جرایمی نظیر پول‌شویی، اختلاس، تقلب، کلاهبرداری و سایر سوءاستفاده‌های مالی و اقتصادی در این حوزه «جرایم بانکی» تعبیر شده است (گسن، ۱۳۹۳: ۵۰)؛ چراکه در متون و نوشتارهای جرم شناختی، اغلب جرایم بانکی در ذیل مصادیق جرایم اقتصادی، جرایم یقه‌سفید، سازمان‌یافته و بدون بزه‌دیده قرار می‌گیرند (میرسعیدی و زمانی، ۱۳۹۲: ۱۶۷).

بزه‌های پولی - بانکی به مجموعه‌ای از رفتارهای غیرقانونی اطلاق می‌شود که در زمینه نظام

۹. جرم اقتصادی رفتار برنامه‌ریزی شده یا سازمان‌یافته توأم با حیله و تقلب است که با هدف تحصیل پول یا مال یا عدم پرداخت وجه یا خسارت یا تحصیل امتیازهایی هنگام فعالیت‌های شغلی ارتکاب می‌یابد. سابقه طرح جرایم اقتصادی در غرب به سال ۱۹۰۵ برمی‌گردد که بُنگر (Bonger, 1916)، بین جرایم خیابانی و جرایم اقتصادی تفکیک قائل شد و پس از آن در سال ۱۹۲۰ ساترلند به مفهوم جرایم یقه‌سفید (White-Collar Crimes) را مطرح کرد.

بانکی و مالی رخ می‌دهد و به‌طور معمول شامل کلاهبرداری، پول‌شویی، اختلاس و سایر جرایم مالی است. این بزه‌ها به دلیل تأثیرات منفی آنها بر اقتصاد و جامعه از اهمیت ویژه‌ای برخوردارند. به‌طور کلی بزه‌های پولی - بانکی را می‌توان به دو دسته اصلی تقسیم کرد: بزه‌های سنتی و بزه‌های نوظهور. بزه‌های سنتی شامل رفتارهایی هستند که در گذشته نیز وجود داشته‌اند، مانند کلاهبرداری‌های بانکی و اختلاس. در مقابل بزه‌های نوظهور به رفتارهایی اطلاق می‌شود که با پیشرفت فناوری و ظهور ابزارهای مالی جدید شکل گرفته‌اند. این بزه‌ها به‌طور معمول پیچیده‌تر و دشوارتر برای شناسایی و نیازمند سیاست‌های جنایی خاص برای مقابله با آنها هستند.

ویژگی‌های اصلی این بزه‌ها عبارت‌اند از:

۱. ماهیت غیرملموس و دیجیتال: برخلاف بسیاری از جرایم سنتی، بزه‌های پولی - بانکی بیشتر در قالب تبادلات دیجیتال و غیرملموس رخ می‌دهند و مجرمان اغلب نیازی به حضور فیزیکی در محل ارتکاب جرم ندارند (Gottschalk, 2018).
۲. پیچیدگی فنی و تخصصی: این جرایم به‌طور معمول مستلزم دانش تخصصی در زمینه بانکداری، فناوری اطلاعات و قوانین مالی و مرتکبین آنها اغلب افرادی با مهارت‌های بالا در این حوزه‌ها هستند (Marr, 2019).
۳. فرامرزی بودن: بسیاری از این جرایم از طریق شبکه‌های بانکی بین‌المللی و ابزارهای دیجیتال رخ می‌دهند و ردیابی آنها فراتر از مرزهای یک کشور را ضروری می‌سازد (Zabyelina & Van Uhm, 2020).
۴. پنهان‌کاری و عدم شفافیت: مرتکبان بزه‌های پولی - بانکی به‌طور معمول از ابزارهای پیچیده‌ای برای پنهان‌سازی هویت خود و ردگیری فعالیت‌های غیرقانونی استفاده می‌کنند از جمله حساب‌های بانکی ناشناس، شرکت‌های پوششی و رمزارزها (FATF, 2021).
۵. ارتباط نزدیک با فساد مالی: بسیاری از این جرایم در بستر فساد سامانمند رخ می‌دهند و مقامات دولتی، بانک‌ها و مؤسسات مالی ممکن است در وقوع یا تسهیل آنها نقش داشته باشند (Rose-Ackerman & Palifka, 2016).
۶. غیرمادی بودن: بسیاری از این بزه‌ها به‌صورت غیرمادی و از طریق فضای مجازی انجام می‌شوند که شناسایی و پیگرد قانونی آنها را دشوار می‌کند.
۷. تأثیرات گسترده: این بزه‌ها نه‌تنها بر قربانیان مستقیم تأثیر می‌گذارند، بلکه می‌توانند به کل نظام اقتصادی آسیب برسانند.

۲-۲- مفهوم و مصادیق سوءاستفاده از فناوری‌های مالی در نظام بانکی

فناوری‌های مالی به کاربرد نوآورانه فناوری در ارائه خدمات مالی گفته می‌شود که از طریق ابزارهایی مانند بانکداری الکترونیکی، پرداخت‌های دیجیتال، رمزارزها، قراردادهای هوشمند و وام‌های هم‌تا به هم‌تا^{۱۰} اجرا می‌شوند (Amer et al., 2016). این فناوری‌ها هرچند به بهبود کارایی و کاهش هزینه‌های سیستم مالی کمک کرده‌اند، اما هم‌زمان چالش‌های جدیدی را برای سیاست‌های جنایی و نظارت بانکی ایجاد کرده‌اند. مصادیق سوءاستفاده از فناوری‌های مالی در نظام بانکی شامل موارد زیر است:

۱. پول‌شویی دیجیتال: مجرمین از ابزارهای دیجیتال مانند کیف پول‌های رمزارزی، صرافی‌های غیرمتمرکز^{۱۱} و پلتفرم‌های پرداخت ناشناس برای انتقال و پنهان‌سازی عواید حاصل از جرایم استفاده می‌کنند (FATF, 2022).
۲. فیشینگ و کلاهبرداری مالی: هکرها و مجرمین سایبری از تکنیک‌های فیشینگ برای دسترسی غیرمجاز به اطلاعات بانکی و سرقت وجوه مشتریان استفاده می‌کنند (Aldawood & Skinner, 2019).
۳. تأمین مالی تروریسم از طریق رمزارزها^{۱۲}: گروه‌های تروریستی از ارزهای دیجیتال برای جمع‌آوری و انتقال پول بدون نظارت‌های بانکی سنتی استفاده می‌کنند (Carlisle, 2021).
۴. دور زدن تحریم‌های مالی: برخی کشورها و سازمان‌ها از فناوری‌های بلاکچین و رمزارزها برای دور زدن تحریم‌های بین‌المللی استفاده می‌کنند (Zarate, 2019).
۵. دست‌کاری بازارهای مالی: از طریق استفاده از الگوریتم‌های معاملاتی و شیوه‌های کلاهبرداری دیجیتال، برخی شرکت‌ها و افراد اقدام به دست‌کاری قیمت سهام، ارزهای دیجیتال و سایر دارایی‌های مالی می‌کنند (Gandal et al., 2018).
۶. کلاهبرداری آنلاین: استفاده از روش‌های مختلف برای فریب کاربران و دسترسی به اطلاعات مالی آنها مانند فیشینگ و کلاهبرداری از طریق ایمیل.
۷. اختلاس اطلاعات: دسترسی غیرمجاز به اطلاعات مشتریان و استفاده از آنها برای انجام فعالیت‌های غیرقانونی.

10. P2P

11. DEX

۱۲. رمزارز، ارزی است که بر بستر بلاکچین یا یک محیط رمزنگاری شده ایجاد شده است. رمزارزها بر اساس فرایندی تحت عنوان ماینینگ تولید می‌شوند، در حالی که ارزهای دیجیتال لزوماً چنین نیستند. لذا هر ارز دیجیتالی لزوماً رمزارز نیست. اما هر رمزارزی یک ارز دیجیتال است (قاسمی، ۱۴۰۰).

این مصادیق نشان می‌دهند که چگونه فناوری‌های مالی می‌توانند به ابزاری برای ارتکاب بزه‌های پولی - بانکی تبدیل شوند.

۲-۳- ارتباط فناوری‌های مالی با بزه‌های نوظهور اقتصادی

تحولات فناوری‌های مالی، منجر به ظهور انواع جدیدی از بزه‌های اقتصادی شده است که چالش‌های حقوقی و سیاست‌گذاری متعددی را به دنبال دارد. با توجه به اینکه این فناوری‌ها امکان انجام تراکنش‌های سریع و آسان را فراهم می‌کنند، مجرمین نیز می‌توانند از این ویژگی‌ها سوءاستفاده کنند. برخی از مهم‌ترین این بزه‌ها عبارت‌اند از:

۱. کلاهبرداری از طریق عرضه اولیه رمزارزها^{۱۳}: بسیاری از پروژه‌های رمزارزی بدون پشتوانه واقعی از طریق عرضه اولیه توکن اقدام به جمع‌آوری سرمایه از مردم کرده و سپس سرمایه‌گذاران را رها می‌کنند (Momtaz, 2020).
۲. سوءاستفاده از قراردادهای هوشمند: قراردادهای هوشمند در بستر بلاکچین اگرچه امکان انجام تراکنش‌های خودکار را فراهم می‌کنند، اما می‌توانند هدف حملات هکری و کلاهبرداری قرار گیرند (Werbach, 2018).
۳. بدافزارهای استخراج رمزارز: مجرمین از بدافزارهای خاصی برای استفاده غیرمجاز از توان پردازشی سیستم‌های کاربران جهت استخراج رمزارز استفاده می‌کنند (Kumar et al., 2019).
۴. تجارت غیرقانونی در دارک وب: بازارهای غیرقانونی که از رمزارزها برای خریدوفروش کالاهای ممنوعه مانند مواد مخدر، اسلحه و اطلاعات سرقت شده استفاده می‌کنند، چالشی جدی برای نهادهای نظارتی ایجاد کرده‌اند (Martin, 2014).
۵. تراکنشات غیرمجاز: استفاده از فناوری برای انجام تراکنشات غیرمجاز بدون اطلاع صاحب حساب.
۶. حملات سایبری: حملات به سیستم‌های بانکی و مالی با هدف سرقت اطلاعات و دارایی‌ها.

درنهایت ارتباط تنگاتنگ بین فناوری‌های مالی و بزه‌های نوظهور اقتصادی، نشان‌دهنده نیاز به سیاست‌های جنایی مؤثر برای مقابله با این چالش‌ها است.

۲-۴- تأثیر این بزه‌ها بر اقتصاد جهانی و ملی

این جرایم نه تنها امنیت مالی کشورها را تهدید می‌کنند، بلکه تأثیرات گسترده‌ای بر ثبات

اقتصادی، افزایش تورم، کاهش اعتماد عمومی به نظام بانکی و افزایش هزینه‌های نظارت مالی دارند. به همین دلیل بسیاری از کشورهای در حال توسعه قوانین و سیاست‌های جدید برای کنترل این جرایم و کاهش تأثیرات منفی آنها بر اقتصاد در نظر گرفتند (OECD, 2022).

۳- سیاست جنایی ایران در قبال بزه‌های پولی - بانکی

بزه‌های پولی - بانکی یکی از چالش‌های اساسی در نظام مالی و اقتصادی ایران محسوب می‌شوند. گسترش فناوری‌های مالی و افزایش پیچیدگی جرایم مرتبط، موجب شده است که سیاست‌های جنایی ایران در ابعاد مختلف تقنینی، قضایی و اجرایی به منظور کنترل، پیشگیری و مقابله با این بزه‌ها توسعه یابند. در این بخش سیاست‌های جنایی ایران در این حوزه بررسی شده و نقاط ضعف و قوت آن تحلیل می‌شود.

۳-۱- سیاست جنایی تقنینی: قوانین و مقررات مرتبط با تخلفات پولی - بانکی

سیاست جنایی تقنینی ایران در زمینه بزه‌های پولی - بانکی از طریق مجموعه‌ای از قوانین و مقررات تدوین شده است که بر اساس استانداردهای بین‌المللی و الزامات داخلی تنظیم شده‌اند.

۳-۱-۱- قانون پولی و بانکی کشور

قانون پولی و بانکی کشور مصوب ۱۳۵۱ به عنوان یکی از مهم‌ترین قوانین در حوزه نظام پولی و بانکی ایران شناخته می‌شود. این قانون ساختار و وظایف بانک مرکزی جمهوری اسلامی ایران را تعیین کرده و به تنظیم نظام پولی و اعتباری کشور می‌پردازد. ماده ۱ این قانون، واحد پول ایران را ریال تعیین کرده و ماده ۱۱ به بانک مرکزی اجازه می‌دهد تا در چهارچوب سیاست‌های پولی، اعتباری و ارزی کشور، نظارت و کنترل لازم را اعمال کند.

۳-۱-۲- قانون مبارزه با پول‌شویی

یکی از مهم‌ترین قوانین مرتبط، قانون مبارزه با پول‌شویی مصوب ۱۳۸۶ و اصلاحیه آن در سال ۱۳۹۷ است که با هدف جلوگیری از ورود عواید حاصل از جرایم به چرخه اقتصاد رسمی تدوین شده است (قانون مبارزه با پول‌شویی، ۱۳۸۶). این قانون، مؤسسات مالی را مکلف به گزارش‌دهی تراکنش‌های مشکوک کرده و برای عدم رعایت مقررات، مجازات‌های مختلفی از جمله جریمه‌های سنگین و انسداد حساب‌های بانکی در نظر گرفته است.

۳-۱-۳- قانون مبارزه با تأمین مالی تروریسم

این قانون که در سال ۱۳۹۴ تصویب شد، به مقابله با تأمین مالی گروه‌های تروریستی و جلوگیری از سوءاستفاده از سیستم بانکی ایران در این زمینه می‌پردازد (قانون مبارزه با تأمین مالی

تروریسم، ۱۳۹۴). طبق این قانون هرگونه تأمین مالی مستقیم یا غیرمستقیم برای فعالیت‌های تروریستی جرم‌انگاری شده و مشمول مجازات‌های شدید است.

۳-۱-۴- قوانین مرتبط با تخلفات بانکی و ارزی

قوانین مرتبط با تخلفات بانکی و ارزی عبارت‌اند از:

- قانون مجازات اخلاگران در نظام اقتصادی کشور (۱۳۶۹): این قانون، مصادیق مختلف تخلفات پولی - بانکی شامل جعل اسناد بانکی، پول‌شویی، قاچاق ارز و سایر جرایم اقتصادی را معرفی کرده و مجازات‌های سنگینی برای مرتکبین در نظر گرفته است.
 - آیین‌نامه اجرایی مبارزه با پول‌شویی (۱۳۹۸): این آیین‌نامه به منظور شفاف‌سازی روند اجرایی قانون مبارزه با پول‌شویی تصویب شده و بانک‌ها را ملزم به رعایت دستورالعمل‌های مرتبط با شناسایی مشتریان و گزارش‌دهی تراکنش‌های مشکوک کرده است.
 - قانون جرایم رایانه‌ای: این قانون که در سال ۱۳۸۸ تصویب شد، به تبیین جرایم مرتبط با فناوری اطلاعات و ارتباطات پرداخته و شامل جرم‌هایی مانند کلاهبرداری اینترنتی و دسترسی غیرمجاز به داده‌ها می‌شود (قانون جرایم رایانه‌ای، ۱۳۸۸).
 - قانون بانکداری بدون ربا: این قانون به‌عنوان مبنای فعالیت بانک‌ها در ایران بر اساس اصول اسلامی تنظیم شده و شامل مقرراتی است که به تخلفات مالی و بانکی نیز پرداخته است (قانون بانکداری بدون ربا، ۱۳۶۲).
- درحالی‌که قوانین تقنینی ایران تا حدی در راستای مبارزه با بزه‌های پولی - بانکی تدوین شده‌اند، اما برخی نواقص ازجمله عدم هماهنگی کامل با استانداردهای بین‌المللی (مانند توصیه‌های FATF) و ضعف در اجرای قوانین وجود دارد که نیازمند اصلاح و به‌روزرسانی است.

۳-۲- سیاست جنایی قضایی: رویه‌های دادگاه‌ها در مواجهه با تخلفات پولی - بانکی

سیاست جنایی قضایی به نحوه برخورد دستگاه قضایی با بزه‌های پولی - بانکی اشاره دارد. این سیاست شامل رویه‌های دادگاه‌ها، نحوه رسیدگی به پرونده‌ها و نوع مجازات‌ها است.

۳-۲-۱- شعب ویژه رسیدگی به جرایم اقتصادی

به‌منظور تسریع در رسیدگی به جرایم پولی - بانکی در قوه قضاییه ایران، شعب ویژه رسیدگی به جرایم اقتصادی تشکیل شده‌اند که وظیفه بررسی پرونده‌های کلان اقتصادی و تخلفات مالی را

بر عهده دارند. این شعب با همکاری نهادهای نظارتی همچون بانک مرکزی و سازمان بازرسی کل کشور اقدام به بررسی پرونده‌های مهم می‌کنند.

۳-۲-۲- احکام صادره در پرونده‌های کلان پولی - بانکی

در سال‌های اخیر، احکام قضایی مهمی علیه جرایم اقتصادی مرتبط با تخلفات بانکی صادر شده است. به‌عنوان مثال پرونده فساد سه هزار میلیاردی که یکی از بزرگ‌ترین پرونده‌های پولی - بانکی ایران بود، منجر به صدور احکام سنگینی از جمله اعدام و حبس‌های طولانی‌مدت برای متهمین شد (دادستانی کل کشور، ۱۳۹۷).

۳-۲-۳- چالش‌های سیاست جنایی قضایی ایران

سیاست جنایی قضایی ایران در رسیدگی به بزه‌های پولی - بانکی با چالش‌هایی همچون طولانی بودن فرایند دادرسی، ضرورت تخصص‌گرایی قضات و فقدان رویه قضایی واحد مواجه است که کارآمدی نظام عدالت کیفری را تحت تأثیر قرار می‌دهد.

- تأخیر در رسیدگی به پرونده‌ها: یکی از مشکلات اصلی زمان‌بر بودن رسیدگی به جرایم اقتصادی در دادگاه‌ها است که موجب تأخیر در اجرای عدالت می‌شود.
- عدم تخصص کافی برخی قضات: با توجه به پیچیدگی جرایم پولی - بانکی برخی قضات تخصص کافی در این حوزه ندارند که این امر می‌تواند منجر به تفسیرهای نادرست از قوانین شود.
- نبود رویه قضایی منسجم: نبود رویه قضایی یکپارچه در برخورد با تخلفات پولی - بانکی منجر به صدور آرای متفاوت در پرونده‌های مشابه شده است.

۳-۳- سیاست جنایی اجرایی: نقش نهادهای نظارتی و بانک مرکزی در کنترل بزه‌های مالی

سیاست جنایی اجرایی به اقداماتی اشاره دارد که نهادهای مختلف برای پیشگیری و کنترل بزه‌های مالی انجام می‌دهند. در ایران نهادهای نظارتی و بانک مرکزی نقش کلیدی در این زمینه دارند.

۳-۳-۱- بانک مرکزی و نظارت بر نظام بانکی

بانک مرکزی ایران، نقش اساسی در نظارت بر مؤسسات مالی و جلوگیری از تخلفات پولی - بانکی ایفا می‌کند. اقدامات بانک مرکزی در این حوزه شامل موارد زیر است:

- الزام بانک‌ها به رعایت مقررات مبارزه با پول‌شویی: بانک مرکزی از طریق ابلاغ دستورالعمل‌های مختلف بانک‌ها را موظف به شناسایی مشتریان، پایش تراکنش‌های مشکوک و گزارش دهی آنها کرده است.

- کنترل نقل و انتقالات مالی: با هدف جلوگیری از خروج غیرقانونی ارز، بانک مرکزی اقداماتی از جمله محدودیت در تراکنش های ارزی و کنترل سخت گیرانه حواله های بانکی انجام داده است.
- نظارت بر بانک ها: بانک مرکزی مسئول نظارت بر فعالیت های بانک ها و مؤسسات مالی است تا از رعایت قوانین و مقررات اطمینان حاصل کند (گزارش سالانه بانک مرکزی، ۱۴۰۰).
- صدور مجوزها: این نهاد، مجوزهای لازم برای تأسیس بانک ها و مؤسسات مالی را صادر کرده و بر عملکرد آنها نظارت می کند (قانون بانکداری بدون ربا، ۱۳۶۲).
- آموزش و آگاهی بخشی: بانک مرکزی اقداماتی را برای آموزش کارکنان بانک ها و افزایش آگاهی عمومی درباره بزه های مالی انجام می دهد.

۳-۳-۲- شورای پول و اعتبار

شورای پول و اعتبار یکی از ارکان کلیدی بانک مرکزی جمهوری اسلامی ایران است که در اجرای سیاست های پولی و اعتباری نقش مؤثری دارد. این شورا بر اساس ماده ۱۸ قانون پولی و بانکی کشور مصوب ۱۳۵۱ تشکیل شده و وظایفی نظیر تصویب مقررات لازم برای تنظیم بازار پول و اعتبار، نظارت بر عملکرد بانک ها و مؤسسات اعتباری و اتخاذ تدابیر لازم برای پیشگیری از بزه های پولی - بانکی را بر عهده دارد (قانون پولی و بانکی کشور، ۱۳۵۱). اقدامات این شورا در مقابله با تخلفات بانکی عبارت اند از:

- تدوین مقررات ضد پول شویی: این شورا در چهارچوب قانون مبارزه با پول شویی مصوب ۱۳۸۶، نقش مهمی در اجرای استانداردهای ضد پول شویی از طریق تصویب مقررات لازم دارد.
- نظارت بر عملکرد بانک ها: نظارت بر رعایت مقررات پولی و بانکی و برخورد با تخلفات از وظایف این شورا است.
- تدوین ضوابط نظارتی در حوزه فناوری های مالی: با گسترش فین تک ها و بانکداری دیجیتال، شورا مقرراتی در جهت کنترل و نظارت بر این حوزه ها تصویب کرده است.

۳-۳-۳- واحد اطلاعات مالی و نقش آن در شناسایی جرایم پولی - بانکی

واحد اطلاعات مالی^{۱۴} زیر نظر وزارت اقتصاد و دارایی فعالیت می کند و وظیفه جمع آوری، تحلیل

و تبادل اطلاعات مرتبط با تخلفات مالی را دارد. این واحد در هماهنگی با بانک‌ها و مؤسسات مالی به شناسایی تراکنش‌های غیرقانونی پرداخته و گزارش‌های خود را به مراجع قضایی ارائه می‌دهد. وظایف و اقدامات این واحد عبارت‌اند از:

- دریافت، تحلیل و پردازش گزارش‌های مشکوک: بانک‌ها و مؤسسات مالی موظف‌اند هرگونه تراکنش مشکوک را به این مرکز گزارش دهند.
- ایجاد سامانه‌های نظارتی هوشمند: توسعه سامانه‌های اطلاعاتی برای کشف جرایم مالی و تحلیل الگوهای پول‌شویی از اقدامات مهم این مرکز است (مرکز اطلاعات مالی و مبارزه با پول‌شویی، ۱۴۰۲).

۳-۳-۴- سایر نهادهای نظارتی مرتبط

سایر نهادهای نظارتی مرتبط عبارت‌اند از:

- سازمان بازرسی کل کشور: مسئول نظارت بر عملکرد مؤسسات مالی و شناسایی تخلفات بانکی است. سازمان بازرسی کل کشور بر اساس اصل ۱۷۴ قانون اساسی جمهوری اسلامی ایران، وظیفه نظارت بر حسن اجرای قوانین در دستگاه‌های دولتی از جمله بانک‌ها و مؤسسات مالی را بر عهده دارد. این سازمان تخلفات بانکی را بررسی کرده و در صورت لزوم تخلفات را به مراجع قضایی ارجاع می‌دهد. نمونه‌ای از اقدامات سازمان بازرسی کل کشور عبارت است از:
 ۱- بررسی پرونده‌های فساد بانکی در چند سال اخیر: این سازمان در پرونده‌های فساد مالی گسترده از جمله پرونده‌های مربوط به وام‌های کلان غیرقانونی نقش داشته است.
- ۲- نظارت بر اجرای سیاست‌های پولی و اعتباری: تطبیق عملکرد بانک‌ها با مقررات شورای پول و اعتبار و بانک مرکزی از جمله اقدامات نظارتی این سازمان است (سازمان بازرسی کل کشور، ۱۴۰۲).
- پلیس فتا: این نهاد در شناسایی و مقابله با تخلفات سایبری مرتبط با جرایم پولی - بانکی نقش مؤثری ایفا می‌کند (گزارش عملکرد پلیس فتا، ۱۴۰۱). با توسعه بانکداری دیجیتال و ظهور فناوری‌های نوین مالی پلیس فضای تولید و تبادل اطلاعات (فتا) نقش اساسی در مبارزه با بزه‌های پولی - بانکی ایفا می‌کند. پلیس فتا بر اساس قانون جرایم رایانه‌ای مصوب ۱۳۸۸، مسئولیت شناسایی و برخورد با تخلفات سایبری از جمله فیشینگ، کلاهبرداری اینترنتی و هک حساب‌های بانکی را بر عهده دارد. برخی اقدامات فتا در مقابله با جرایم بانکی عبارت‌اند از:
 ۱- ایجاد سامانه‌های هشدار سریع برای بانک‌ها و مشتریان: این سامانه‌ها به

شهروندان کمک می‌کند تا از تهدیدات احتمالی در فضای بانکی دیجیتال آگاه شوند. ۲- ردیابی و انهدام شبکه‌های فیشینگ و کلاهبرداری اینترنتی: پلیس فتا در سال‌های اخیر چندین باند فیشینگ که از طریق سوءاستفاده از اطلاعات کارت‌های بانکی اقدام به سرقت از حساب‌ها کرده بودند را شناسایی و منهدم کرده است (پلیس فتا، ۱۴۰۲).

- سازمان بورس و اوراق بهادار: این سازمان مسئول نظارت بر بازار سرمایه بوده و اقداماتی را برای جلوگیری از تخلفات مالی در این حوزه انجام می‌دهد (گزارش سالانه سازمان بورس، ۱۴۰۰).

باوجود تلاش‌های بانک مرکزی و سایر نهادهای نظارتی، ضعف‌هایی به شرح زیر در اجرای سیاست‌های اجرایی وجود دارد:

- عدم دسترسی به اطلاعات مالی شفاف: برخی مؤسسات مالی از ارائه اطلاعات دقیق خودداری کرده که باعث کاهش اثربخشی نظارت می‌شود.
- عدم همکاری کافی بین نهادهای نظارتی و اجرایی: هماهنگی بین بانک مرکزی، واحد اطلاعات مالی و دستگاه قضایی نیازمند تقویت است.
- کمبود منابع انسانی متخصص: بسیاری از نهادهای نظارتی با کمبود نیروی انسانی متخصص مواجه هستند که این موضوع می‌تواند بر کیفیت نظارت تأثیر منفی بگذارد.

سیاست جنایی ایران در قبال بزه‌های پولی - بانکی از سه بُعد تقنینی، قضایی و اجرایی مورد بررسی قرار گرفته است. در بعد تقنینی، قوانین مرتبط با مبارزه با پول‌شویی و تأمین مالی تروریسم به تصویب رسیده‌اند، اما نیاز به اصلاح و هماهنگی با استانداردهای بین‌المللی دارند. در بعد قضایی، شعب ویژه برای رسیدگی به جرایم مالی تشکیل شده، اما مشکلاتی نظیر تأخیر در دادرسی و نبود رویه یکپارچه وجود دارد. در بعد اجرایی، بانک مرکزی و نهادهای نظارتی در مقابله با تخلفات مالی نقش ایفا می‌کنند، اما چالش‌هایی مانند ضعف شفافیت مالی و عدم هماهنگی کافی بین نهادها مشهود است. اصلاح قوانین، افزایش تخصص قضات و تقویت نظارت مالی ازجمله راهکارهای بهبود سیاست جنایی ایران در این حوزه هستند.

۴- سوءاستفاده از فناوری‌های مالی در نظام بانکی ایران

فناوری‌های مالی با ارائه راهکارهای نوین، تحول شگرفی در نظام بانکی و مالی ایجاد کرده‌اند. این فناوری‌ها با تسهیل تراکنش‌ها، افزایش دسترسی به خدمات مالی و کاهش هزینه‌ها، مزایای قابل توجهی به همراه داشته‌اند. با این حال همین پیشرفت‌ها، زمینه‌ساز سوءاستفاده‌هایی نیز شده‌اند که

می‌توانند ثبات و امنیت نظام بانکی را به خطر بیندازند. در این بخش به تحلیل موارد سوءاستفاده از فناوری‌های مالی در ایران، خلأهای قانونی و چالش‌های حقوقی در پیشگیری و برخورد با این جرایم و نقش بانک‌ها، فین‌تک‌ها و مؤسسات مالی در پیشگیری از تخلفات پرداخته می‌شود.

۴-۱- تحلیل موارد سوءاستفاده از فناوری‌های مالی در کشور

فناوری‌های مالی به‌عنوان یکی از نوآوری‌های مهم در عرصه خدمات مالی و بانکی در سال‌های اخیر در ایران نیز رشد چشمگیری داشته‌اند. با این حال این پیشرفت‌ها به همراه خود چالش‌ها و خطرات جدیدی را به وجود آورده است. سوءاستفاده از فناوری‌های مالی به معنای بهره‌برداری نادرست یا غیرقانونی از این فناوری‌ها برای انجام فعالیت‌های مجرمانه است.

۴-۱-۱- کلاهبرداری‌های الکترونیکی و فیشینگ

با گسترش بانکداری الکترونیکی، کلاهبرداری‌های مرتبط با فیشینگ افزایش یافته است. در این روش مهاجمین با ایجاد وب‌سایت‌ها یا ارسال پیام‌های جعلی اطلاعات محرمانه کاربران را به دست آورده و از حساب‌های بانکی آنها سوءاستفاده می‌کنند. عدم آگاهی کافی کاربران و نبود سیستم‌های احراز هویت قوی، این نوع کلاهبرداری را تسهیل کرده است. طبق گزارش پلیس فتا طی سال‌های اخیر تعداد این نوع کلاهبرداری‌ها به طرز قابل توجهی افزایش یافته است (گزارش عملکرد پلیس فتا، ۱۴۰۱). به‌عنوان مثال کلاهبرداران با ایجاد وب‌سایت‌های جعلی و تقلید از برندهای معتبر اقدام به جمع‌آوری اطلاعات شخصی و مالی کاربران می‌کنند.

۴-۱-۲- سوءاستفاده از دستگاه‌های پرداخت غیرنقدی

دستگاه‌های پرداخت غیرنقدی^{۱۵} که برای تسهیل پرداخت‌ها طراحی شده‌اند، در برخی موارد مورد سوءاستفاده قرار گرفته‌اند. برخی افراد با استفاده از این دستگاه‌ها و بهره‌گیری از خلأهای نظارتی، اقدام به فرار مالیاتی یا پول‌شویی کرده‌اند. این مسئله نشان‌دهنده نیاز به نظارت دقیق‌تر بر این دستگاه‌ها و تراکنش‌های مرتبط با آنهاست.

۴-۱-۳- پول‌شویی

پول‌شویی یکی دیگر از خطرات مرتبط با فناوری‌های مالی است. با توجه به اینکه فناوری‌های مالی امکان انجام تراکنش‌ها به‌صورت سریع و بدون نیاز به حضور فیزیکی را فراهم می‌کنند، این موضوع بستر مناسبی برای فعالیت‌های پول‌شویی ایجاد کرده است. بر اساس گزارش بانک مرکزی برخی از بزهکاران از طریق سیستم‌های پرداخت الکترونیکی و ارزهای دیجیتال اقدام به

انتقال وجوه غیرقانونی می‌کنند (گزارش سالانه بانک مرکزی، ۱۴۰۰).

۴-۱-۴- جرایم مرتبط با ارزهای دیجیتال

ارزهای دیجیتال به دلیل ماهیت غیرمتمرکز و ناشناس بودن تراکنش‌ها، زمینه‌ساز جرایم مالی متعددی شده‌اند. در ایران خلأهای حقوقی در حوزه ارزهای دیجیتال راه را برای سوءاستفاده باز گذاشته است. عدم تدوین قوانین مشخص در این حوزه باعث شده تا برخی افراد با استفاده از این ارزها اقدام به پول‌شویی، تأمین مالی فعالیت‌های غیرقانونی و فرار مالیاتی کنند.

۴-۱-۵- جرایم سایبری

جرایم سایبری نیز به‌عنوان یکی دیگر از ابعاد سوءاستفاده از فناوری‌های مالی مطرح هستند. این جرایم شامل هک کردن حساب‌های بانکی، دسترسی غیرمجاز به اطلاعات مشتریان و تخریب داده‌ها می‌شود. طبق آمارهای موجود در سال ۱۴۰۰ تعداد جرایم سایبری نسبت به سال‌های گذشته افزایش یافته است.

۴-۲- خلأهای قانونی و چالش‌های حقوقی در پیشگیری و برخورد با این جرایم

باوجود تلاش‌های صورت‌گرفته برای مقابله با سوءاستفاده از فناوری‌های مالی، هنوز هم خلأهای قانونی و چالش‌های حقوقی متعددی وجود دارد که کارایی اقدامات پیشگیرانه را تحت تأثیر قرار می‌دهد.

۴-۲-۱- نبود قوانین جامع و به‌روز

سرعت بالای پیشرفت فناوری‌های مالی باعث شده است که قوانین موجود نتوانند پاسخگوی چالش‌های جدید باشند. برای مثال در حوزه ارزهای دیجیتال قوانین مشخصی برای نظارت، گرفتن مالیات و برخورد با تخلفات وجود ندارد. این خلأ قانونی امکان سوءاستفاده را افزایش داده و نظارت مؤثر را دشوار کرده است.

۴-۲-۲- تعدد نهادهای نظارتی و عدم هماهنگی بین آنها

در ایران چندین نهاد مسئول نظارت بر نظام بانکی و مالی هستند، اما عدم هماهنگی بین آنها باعث شده است که در برخی موارد، جرایم مالی به‌درستی شناسایی و پیگیری نشوند. این تعدد و تداخل وظایف، کارایی سیستم نظارتی را کاهش داده و فرصت‌هایی برای سوءاستفاده کنندگان ایجاد کرده است.

۴-۲-۳- ضعف در تعریف و تشخیص جرایم مالی نوظهور

بسیاری از جرایم مرتبط با فناوری‌های مالی، مانند کلاهبرداری‌های پیچیده دیجیتال در قوانین

سنتی تعریف نشده‌اند. این موضوع باعث شده است که دستگاه قضایی در تشخیص و برخورد با این جرایم با چالش مواجه شود. ضرورت دارد که قوانین موجود بازنگری شده و تعاریف جدیدی برای جرایم مالی نوظهور ارائه شود.

۴-۲-۴- عدم تطابق قوانین با فناوری‌های نوین

یکی از بزرگ‌ترین چالش‌ها، عدم تطابق قوانین موجود با فناوری‌های نوین است. بسیاری از قوانین فعلی در زمینه جرایم مالی و سایبری مربوط به دوران قبل از ظهور فناوری‌های نوین هستند و نمی‌توانند به‌طور کامل نیازهای کنونی را پاسخگو باشند. به‌عنوان مثال، قوانین مربوط به کلاهبرداری و پول‌شویی نیازمند بازنگری هستند تا بتوانند با روش‌های جدید سوءاستفاده همخوانی داشته باشند.

۴-۲-۵- مشکلات بین‌المللی

چالش دیگری که در زمینه سوءاستفاده از فناوری‌های مالی وجود دارد، مشکلات بین‌المللی است. با توجه به اینکه بسیاری از فعالیت‌ها در فضای مجازی انجام می‌شوند، پیگیری و شناسایی بزه‌کاران در سطح بین‌المللی دشوار است. همچنین تحریم‌ها و محدودیت‌های بین‌المللی نیز بر توانایی ایران در همکاری با سایر کشورها برای مبارزه با جرایم سایبری تأثیر منفی گذاشته است.

۴-۳- نقش بانک‌ها، فین‌تک‌ها و مؤسسات مالی در پیشگیری از تخلفات

بانک‌ها و مؤسسات مالی به‌عنوان بازیگران اصلی در نظام مالی کشور نقش کلیدی در پیشگیری از سوءاستفاده از فناوری‌های مالی دارند.

۴-۳-۱- توسعه سیستم‌های نظارتی پیشرفته

بانک‌ها و مؤسسات مالی باید با بهره‌گیری از فناوری‌های نوین، سیستم‌های نظارتی خود را تقویت کنند. استفاده از الگوریتم‌های هوش مصنوعی و یادگیری ماشین می‌تواند در شناسایی الگوهای غیرمعمول و کشف تقلب مؤثر باشد. این سیستم‌ها قادرند تراکنش‌های مشکوک را به‌صورت خودکار شناسایی کرده و به واحدهای نظارتی گزارش دهند.

۴-۳-۲- آموزش و افزایش آگاهی مشتریان

یکی از مهم‌ترین راه‌های پیشگیری از کلاهبرداری‌های مالی، افزایش آگاهی مشتریان است. بانک‌ها و فین‌تک‌ها باید برنامه‌های آموزشی منظمی برای مشتریان خود در نظر بگیرند تا آنها را با روش‌های مختلف کلاهبرداری و نحوه محافظت از اطلاعات شخصی آشنا کنند.

۴-۳-۳- همکاری نزدیک با نهادهای قانونگذار

بانک‌ها و فین‌تک‌ها باید با نهادهای قانونگذار همکاری نزدیکی داشته باشند تا بتوانند در تدوین قوانین و مقررات مرتبط با فناوری‌های مالی نقش مؤثری ایفا کنند. این همکاری می‌تواند به ایجاد چهارچوب‌های قانونی مناسب و کاهش خلأهای موجود کمک کند.

۴-۳-۴- پیاده‌سازی استانداردهای امنیتی بالا

استفاده از پروتکل‌های امنیتی پیشرفته و بروز می‌تواند از بسیاری از سوءاستفاده‌ها جلوگیری کند. بانک‌ها و فین‌تک‌ها باید به‌صورت مداوم زیرساخت‌های امنیتی خود را به‌روزرسانی کرده و از استانداردهای بین‌المللی، مانند ISO/IEC 27001 برای مدیریت امنیت اطلاعات و PCI DSS برای ایمن‌سازی تراکنش‌های مالی تبعیت کنند.

علاوه بر این پیاده‌سازی الگوریتم‌های رمزنگاری قوی، استفاده از احراز هویت چندعاملی^{۱۶} و به‌کارگیری فناوری‌های ضد بدافزار و فایروال‌های هوشمند می‌تواند به کاهش ریسک حملات سایبری منجر شود. همچنین توسعه سیستم‌های مانیتورینگ بلادرنگ برای شناسایی تراکنش‌های مشکوک و استفاده از هوش مصنوعی و یادگیری ماشین در تحلیل الگوهای غیرعادی تراکنش‌ها از اقدامات ضروری در راستای افزایش امنیت شبکه‌های بانکی و فین‌تک‌ها محسوب می‌شود. بانک‌ها و شرکت‌های فعال در حوزه فناوری مالی باید سیاست‌های امنیت سایبری سختگیرانه را در دستور کار خود قرار دهند و با بهره‌گیری از نمونه‌های نفوذپذیری دوره‌ای^{۱۷} نقاط ضعف خود را شناسایی و برطرف کنند. همکاری با نهادهای نظارتی و استفاده از چهارچوب‌های قانونی بین‌المللی مانند مقررات عمومی حفاظت از داده‌ها^{۱۸} و کارگروه ویژه اقدام مالی^{۱۹} نیز نقش بسزایی در کاهش جرایم مالی و پول‌شویی ایفا خواهد کرد. درنهایت آموزش مستمر کارکنان و مشتریان درباره تهدیدات امنیتی و شیوه‌های مقابله با آنها یکی از مؤثرترین روش‌ها برای جلوگیری از حملات فیشینگ، مهندسی اجتماعی و سایر شیوه‌های سوءاستفاده از فناوری‌های مالی محسوب می‌شود. سوءاستفاده از فناوری‌های مالی در نظام بانکی ایران یک چالش جدی است که نیازمند توجه ویژه‌ای از سوی قانونگذاران، نهادهای نظارتی و خود بانک‌ها می‌باشد. باوجود تلاش‌هایی که برای مقابله با این مشکلات صورت گرفته است، هنوز هم خلأهای قانونی و چالش‌های اجرایی وجود دارد که باید برطرف شوند. تقویت سیستم‌های امنیتی، آموزش مشتریان و همکاری با نهادهای نظارتی می‌تواند راهکارهایی مؤثر

16. Multi-Factor Authentication (MFA)

17. Penetration Testing

18. General Data Protection Regulation (GDPR)

19. Financial Action Task Force (FATF)

برای کاهش این نوع تخلفات باشد.

۴-۴- تحلیل نمونه‌های واقعی بزه‌های پولی - بانکی مبتنی بر فناوری‌های مالی

بررسی پرونده‌های واقعی در حوزه بزه‌های پولی - بانکی نشان می‌دهد که توسعه فناوری‌های مالی در کنار مزایای اقتصادی، بستر ارتکاب جرایم پیچیده و سازمان‌یافته را نیز فراهم ساخته است. در ایران و نظام‌های حقوقی مورد مطالعه، نمونه‌های متعددی از سوءاستفاده از ابزارهای مالی دیجیتال مشاهده می‌شود که بیانگر ضرورت بازنگری در سیاست‌های جنایی است.

۴-۴-۱- پرونده صرافی رمز ارزی «کریپتولند» در ایران

یکی از مهم‌ترین پرونده‌های مالی مرتبط با فناوری‌های نوین در ایران، پرونده صرافی رمز ارزی «کریپتولند» بود که در سال ۱۴۰۰ منجر به مداخله قضایی و بازداشت مدیران آن شد. در این پرونده، ابهامات گسترده درباره نحوه نگهداری دارایی‌های کاربران، فقدان نظارت قانونی شفاف، احتمال اختلال در نظام اقتصادی و عدم شفافیت تراکنش‌ها مطرح گردید. این پرونده نشان داد که خلأ تقنینی در حوزه رمزارزها و نبود نظام نظارتی تخصصی، می‌تواند موجب بروز بحران‌های مالی گسترده و تضییع حقوق کاربران شود.

۴-۴-۲- پرونده بانک «ولز فارگو» در ایالات متحده آمریکا

در ایالات متحده، بانک ولز فارگو^{۲۰} در سال ۲۰۱۶ به دلیل ایجاد میلیون‌ها حساب بانکی و اعتباری جعلی بدون رضایت مشتریان، با یکی از بزرگ‌ترین رسوایی‌های بانکی مواجه شد. این پرونده منجر به اعمال جرمه‌های سنگین مالی، مداخله نهادهای نظارتی و اصلاح ساختارهای کنترلی بانک گردید. اهمیت این پرونده در آن است که نشان می‌دهد حتی در نظام‌های مالی پیشرفته نیز ضعف نظارت داخلی و انگیزه‌های سودمحور می‌تواند زمینه ارتکاب جرایم مالی گسترده را فراهم سازد.

۴-۴-۳- پرونده پول‌شویی از طریق رمزارزها در اتحادیه اروپا

در سال‌های اخیر، اتحادیه اروپا با پرونده‌های متعددی در زمینه پول‌شویی از طریق رمزارزها و پلتفرم‌های مالی غیرمتمرکز مواجه شده است. برای نمونه در برخی کشورهای اروپایی، شبکه‌هایی شناسایی شدند که از طریق تراکنش‌های رمز ارزی و کیف پول‌های دیجیتال، اقدام به انتقال وجوه ناشی از جرایم سازمان‌یافته و فرار مالیاتی می‌کردند. این موارد موجب شد تا اتحادیه اروپا «دستورالعمل پنجم مبارزه با پول‌شویی» را با تمرکز بر شناسایی هویت کاربران

رمزارزی و افزایش الزامات گزارش دهی تصویب کند.

۴-۴-۴- تحلیل تطبیقی پرونده‌ها

بررسی این پرونده‌ها نشان می‌دهد که بزه‌های مالی فناورانه دارای ویژگی‌هایی نظیر فراملی بودن، پیچیدگی فنی، سرعت بالای انتقال وجوه و دشواری ردیابی هستند. در حالی که اتحادیه اروپا و ایالات متحده با توسعه سامانه‌های هوشمند نظارتی، تقویت همکاری میان نهادهای مالی و بهره‌گیری از فناوری‌های تحلیل داده تا حدی موفق به کنترل این جرایم شده‌اند، در ایران همچنان خلأهای قانونی، ضعف نظارت بر پلتفرم‌های مالی نوین و فقدان چهارچوب‌های شفاف تنظیم‌گری مشاهده می‌شود.

۵- بررسی تطبیقی سیاست‌های جنایی اتحادیه اروپا و ایالات متحده آمریکا در مقابله با بزه‌های پولی - بانکی

بزه‌های پولی - بانکی، به‌عنوان تهدیدی جدی برای نظام‌های مالی و اقتصادی جهان، نیازمند سیاست‌های جنایی مؤثر و هماهنگ در سطح بین‌المللی هستند. اتحادیه اروپا و ایالات متحده آمریکا، به‌عنوان دو نظام حقوقی پیشرو، راهکارها و ساختارهای قانونی متنوعی برای مقابله با این جرایم اتخاذ کرده‌اند. در این بخش به بررسی تطبیقی این سیاست‌ها پرداخته و نقاط قوت و ضعف قوانین ایران را در مقایسه با استانداردهای بین‌المللی مورد ارزیابی قرار می‌دهیم.

۵-۱- ساختارهای حقوقی و مقررات مرتبط با بزه‌های پولی - بانکی در اتحادیه اروپا

اتحادیه اروپا با درک اهمیت مقابله با جرایم مالی به‌ویژه پول‌شویی، چهارچوب‌های قانونی جامعی را تدوین کرده است. این چهارچوب‌ها شامل دستورالعمل‌ها و مقرراتی هستند که کشورهای عضو ملزم به اجرای آنها می‌باشند.

۵-۱-۱- دستورالعمل‌های مبارزه با پول‌شویی

اتحادیه اروپا دارای چندین دستورالعمل و مقرر است که به‌طور خاص به بزه‌های مالی و پولی پرداخته‌اند. یکی از مهم‌ترین این اسناد، دستورالعمل مبارزه با پول‌شویی^{۲۱} است که در چندین نسخه بروز شده و به کشورهای عضو الزام می‌کند تا سیستم‌های نظارتی مؤثری برای شناسایی و پیشگیری از فعالیت‌های پول‌شویی ایجاد کنند (European Commission, 2020). اتحادیه اروپا چندین دستورالعمل برای مبارزه با پول‌شویی تصویب کرده است که مهم‌ترین آنها عبارت‌اند از:

- دستورالعمل چهارم مبارزه با پول‌شویی (۸۴۹/۲۰۱۵): این دستورالعمل بر تقویت

21. Anti-Money Laundering Directive (AMLD)

رویکرد مبتنی بر ریسک، افزایش شفافیت در مالکیت واقعی شرکت‌ها و بهبود همکاری بین‌المللی تأکید دارد.

- دستورالعمل پنجم مبارزه با پول‌شویی (۸۴۳/۲۰۱۸): این اصلاحیه بر دستورالعمل قبلی به موضوعاتی مانند ارزش‌های دیجیتال، کارت‌های پیش‌پرداخت ناشناس و همکاری بین واحدهای اطلاعات مالی پرداخته است.
- دستورالعمل ششم مبارزه با پول‌شویی (۱۱۵۳/۲۰۲۱): این دستورالعمل جدیدترین اقدام اتحادیه اروپا در مقابله با پول‌شویی است که بر هماهنگی بیشتر قوانین کیفری در سراسر اتحادیه و تعیین مجازات‌های سخت‌گیرانه‌تر تمرکز دارد.

۵-۱-۲- نهادهای نظارتی و اجرایی

اتحادیه اروپا با ایجاد نهادهایی نظیر واحد اطلاعات مالی اروپا^{۲۲} و سازمان نظارت بر بانکداری اروپا^{۲۳} به هماهنگی و نظارت بر اجرای قوانین مبارزه با پول‌شویی در کشورهای عضو می‌پردازد. سازمان مبارزه با تقلب اروپایی^{۲۴} و مرکز نظارت بر پول‌شویی از جمله این نهادها هستند که وظیفه نظارت بر رعایت قوانین و شناسایی تخلفات را بر عهده دارند (European Union Agency for Law Enforcement Cooperation, 2021).

۵-۲- اقدامات پیشگیرانه در اتحادیه اروپا

اتحادیه اروپا همچنین بر اهمیت اقدامات پیشگیرانه تأکید دارد. این اقدامات شامل آموزش کارکنان مؤسسات مالی، شناسایی مشتریان و ارزیابی ریسک است. به‌عنوان مثال دستورالعمل مبارزه با پول‌شویی به مؤسسات مالی الزام می‌کند که اطلاعات دقیقی از مشتریان خود جمع‌آوری کنند و هرگونه فعالیت مشکوک را گزارش دهند (European Commission, 2020).

۵-۳- تحلیل قوانین و اقدامات پیشگیرانه در ایالات متحده آمریکا

ایالات متحده نیز بر اهمیت اقدامات پیشگیرانه تأکید دارد. مؤسسات مالی موظفاند تا برنامه‌های شناسایی مشتری را اجرا کنند و هرگونه فعالیت مشکوک را به مقامات گزارش دهند. همچنین آموزش کارکنان درباره خطرات احتمالی و روش‌های شناسایی تخلفات جزء الزامات قانونی است (U.S. Department of the Treasury, 2021). ایالات متحده با سابقه‌ای طولانی در مبارزه با جرایم مالی، مجموعه‌ای از قوانین و اقدامات پیشگیرانه را به کار گرفته است.

22 FIU.net

23. European Banking Authority (EBA)

24. European Anti-Fraud Office (OLAF)

۵-۳-۱- قانون رازداری بانکی

این قانون اولین تلاش جدی آمریکا در مقابله با پول شویی بود که مؤسسات مالی را ملزم به گزارش تراکنش‌های نقدی بزرگ و فعالیت‌های مشکوک می‌کرد. هدف اصلی آن جلوگیری از استفاده از سیستم مالی برای اهداف غیرقانونی است (U.S. Department of the Treasury, 2021).

۵-۳-۲- قانون میهن‌پرستی ایالات متحده مصوب ۲۰۰۱^{۲۵}

پس از حملات ۱۱ سپتامبر، این قانون با هدف تقویت توانایی دولت در شناسایی و جلوگیری از تأمین مالی تروریسم تصویب شد. این قانون، اختیارات نظارتی و تحقیقاتی بیشتری به نهادهای اجرایی داده و مجازات‌های شدیدتری برای جرایم مالی مرتبط با تروریسم تعیین کرده است.

۵-۳-۳- نهادهای نظارتی و اجرایی

در آمریکا نهادهایی مانند شبکه اجرای جرایم مالی^{۲۶} و دفتر کنترل دارایی‌های خارجی^{۲۷} مسئول نظارت بر اجرای قوانین مبارزه با پول شویی و تحریم‌ها هستند. این نهادها با همکاری مؤسسات مالی به شناسایی و مقابله با فعالیت‌های غیرقانونی می‌پردازند. سرویس درآمد داخلی^{۲۸} وابسته به وزارت خزانه‌داری ایالات متحده نیز از جمله این نهادهاست که به‌طور مستقیم با تخلفات مالی مقابله می‌کند (U.S. Department of the Justice, 2020).

۵-۴- مقایسه نقاط قوت و ضعف قوانین ایران در برابر استانداردهای بین‌المللی

ایران نیز در سال‌های اخیر تلاش‌هایی برای مقابله با جرایم مالی انجام داده است، اما در مقایسه با استانداردهای بین‌المللی، چالش‌ها و کاستی‌هایی وجود دارد.

۵-۴-۱- نقاط قوت

پیشرفت‌ها و نقاط قوت قوانین ایران در مقایسه با استانداردهای بین‌المللی عبارت‌اند از:

۱. تصویب قانون مبارزه با پول شویی و اصلاحات آن: یکی از مهم‌ترین پیشرفت‌های ایران در این حوزه تصویب قانون مبارزه با پول شویی مصوب ۱۳۸۶ و اصلاحیه آن در سال ۱۳۹۷ بوده است. این قانون، چهارچوبی قانونی برای مقابله با جریان‌های مالی غیرقانونی تعیین کرده و نهادهای مسئول را مشخص نموده است (قانون مبارزه با پول شویی، ماده ۱). اصلاحات بعدی نیز سازکارهای شفاف‌تری برای

25. USA PATRIOT Act of 2001

26. FinCEN

27. Office of Foreign Assets Control (OFAC)

28. Internal Revenue Service (IRS)

- نظارت بر مؤسسات مالی و تراکنش‌های بانکی ارائه داده‌اند.
۲. تأسیس مرکز اطلاعات مالی و توسعه نظارت مالی: بر اساس ماده ۳ قانون مبارزه با پول‌شویی، مرکز اطلاعات مالی ایران به‌عنوان نهاد ناظر بر فعالیت‌های مالی مشکوک ایجاد شده است. این مرکز به جمع‌آوری و تحلیل اطلاعات مرتبط با تراکنش‌های مشکوک می‌پردازد و در همکاری با بانک‌ها و مؤسسات مالی مانع از سوءاستفاده از سیستم بانکی می‌شود (FIU، گزارش سالانه ۱۴۰۰).
۳. جرم‌انگاری پول‌شویی و تأمین مالی تروریسم: قانون اصلاح قانون مبارزه با پول‌شویی (۱۳۹۷) و قانون مبارزه با تأمین مالی تروریسم (۱۳۹۴)، اقدامات مرتبط با پول‌شویی را جرم‌انگاری کرده و مجازات‌های متناسبی برای آن تعیین کرده‌اند. بر اساس این قوانین، اشخاص حقیقی و حقوقی که در فرایند پول‌شویی یا تأمین مالی فعالیت‌های مجرمانه نقش داشته باشند، تحت پیگرد قضایی قرار خواهند گرفت (ماده ۹ قانون مبارزه با پول‌شویی).
۴. نظارت بیشتر بر تراکنش‌های مالی و فین‌تک‌ها: بانک مرکزی ایران با تصویب مقررات نظارتی بر شرکت‌های فین‌تک و ارائه‌دهندگان خدمات پرداخت، تلاش کرده است تا از سوءاستفاده از فناوری‌های مالی در پول‌شویی جلوگیری کند. این مقررات شامل الزام به احراز هویت مشتریان، ثبت تراکنش‌های مشکوک و گزارش آنها به مرکز اطلاعات مالی می‌شود (بخشنامه بانک مرکزی، ۱۴۰۱).

۵-۴-۲- نقاط ضعف

- علی‌رغم پیشرفت‌های قابل توجه ایران همچنان در برخی زمینه‌ها با چالش‌هایی مواجه است که موجب می‌شود سیاست‌های جنایی آن در حوزه بزه‌های پولی - بانکی کمتر از حد استانداردهای بین‌المللی باشد. مهم‌ترین نقاط ضعف عبارت‌اند از:
۱. عدم انطباق کامل با توصیه‌های گروه ویژه اقدام مالی: ایران همچنان در فهرست کشورهای قرار دارد که از نظر گروه ویژه اقدام مالی در ریسک بالای پول‌شویی و تأمین مالی تروریسم قرار دارند. دلیل اصلی این موضوع، عدم تصویب کامل کنوانسیون مقابله با جرایم سازمان‌یافته فراملی (پالرمو) و کنوانسیون مقابله با تأمین مالی تروریسم است. در حالی که بسیاری از کشورها این الزامات را پذیرفته‌اند، ایران هنوز در برخی موارد از اجرای استانداردهای FATF خودداری کرده است (FATF, 2023).
۲. ضعف در اجرای قوانین و عدم هماهنگی نهادهای نظارتی: باوجود تدوین قوانین مرتبط با پول‌شویی و بزه‌های مالی، اجرای آنها همچنان با چالش‌هایی روبه‌رو است.

عدم هماهنگی میان بانک مرکزی، مرکز اطلاعات مالی، قوه قضائیه و نهادهای اجرایی باعث شده است که نظارت بر تراکنش‌های مالی به‌درستی انجام نشود. این ناهماهنگی موجب تأخیر در پیگیری مجرمین مالی و کاهش کارآمدی سیاست‌های جنایی ایران در این حوزه شده است (گزارش مرکز پژوهش‌های مجلس، ۱۴۰۲).

۳. عدم شفافیت در نظام بانکی و اقتصاد غیررسمی گسترده: یکی از مشکلات اساسی در ایران، حجم بالای اقتصاد غیررسمی و معاملات نقدی بدون نظارت است. بسیاری از تراکنش‌های مالی در ایران بدون ثبت در نظام بانکی انجام می‌شوند که امکان شناسایی فعالیت‌های مشکوک را کاهش می‌دهد. در حالی که در اتحادیه اروپا و آمریکا سقف معینی برای پرداخت‌های نقدی تعیین شده ایران هنوز محدودیت‌های دقیقی در این زمینه اعمال نکرده است (گزارش بانک جهانی، ۲۰۲۳).

۴. نبود قوانین جامع برای مقابله با سوءاستفاده از ارزهای دیجیتال: در حالی که اتحادیه اروپا و ایالات متحده قوانین جامع برای نظارت بر ارزهای دیجیتال و تراکنش‌های مرتبط با آنها وضع کرده‌اند، ایران هنوز چهارچوب قانونی شفاف در این زمینه ندارد. این موضوع باعث شده است که برخی افراد از صرافی‌های غیرمجاز و کیف پول‌های دیجیتال برای انتقال دارایی‌های غیرقانونی استفاده کنند. در حالی که بانک مرکزی ایران برخی دستورالعمل‌ها را در این زمینه صادر کرده، اما هنوز یک قانون جامع برای مبارزه با پول‌شویی از طریق ارزهای دیجیتال در کشور تصویب نشده است (مرکز پژوهش‌های مجلس، ۱۴۰۱).

۵-۵- پیشنهادهایی برای بهبود سیاست‌های جنایی ایران

با توجه به نقاط قوت و ضعف نظام حقوقی ایران در مقایسه با استانداردهای بین‌المللی، پیشنهادهای زیر برای بهبود سیاست‌های جنایی در این حوزه ارائه می‌شود:

۱. پذیرش کامل توصیه‌های FATF و بهبود همکاری‌های بین‌المللی: با تصویب و اجرای کامل کنوانسیون‌های CFT و پالرمو، ایران می‌تواند ریسک‌های مرتبط با پول‌شویی و تأمین مالی تروریسم را کاهش داده و از فهرست کشورهای پرخطر FATF خارج شود. این امر می‌تواند موجب افزایش شفافیت مالی، بهبود روابط بانکی بین‌المللی و تسهیل همکاری‌های قضایی در پرونده‌های پول‌شویی شود.
۲. افزایش نظارت بر معاملات نقدی و تعیین سقف پرداخت‌های غیرالکترونیکی: با توجه به تجارب اتحادیه اروپا، تعیین سقف برای پرداخت‌های نقدی (برای مثال ۱۰ میلیون تومان) می‌تواند شفافیت مالی را افزایش دهد و از فرار مالیاتی و پول‌شویی

جلوگیری کند. اجرای این سیاست همراه با توسعه پرداخت‌های دیجیتال و سیستم‌های احراز هویت تراکنش‌های مالی ضروری است.

۳. تصویب قوانین جامع برای نظارت بر ارزش‌های دیجیتال: ایران باید قوانینی مشابه قانون بازارهای دارایی دیجیتال (MiCA) اتحادیه اروپا تدوین کند که شامل الزامات شفافیت، ثبت صرافی‌های رمزارز، گزارش دهی تراکنش‌های مشکوک و جلوگیری از سوءاستفاده‌های مالی باشد.

۴. بهبود هماهنگی میان نهادهای نظارتی و اجرایی: لازم است یک مرکز هماهنگی ملی برای مبارزه با جرایم پولی - بانکی ایجاد شود که شامل بانک مرکزی، مرکز اطلاعات مالی، قوه قضائیه و پلیس فتا باشد تا اجرای قوانین به‌صورت مؤثرتر انجام شود.

۵. هماهنگی با استانداردهای بین‌المللی: بازنگری و اصلاح قوانین برای تطبیق با توصیه‌های FATF و سایر استانداردهای بین‌المللی ضروری است.

مبارزه با بزه‌های پولی - بانکی نیازمند یک رویکرد جامع و هماهنگ است که شامل تدوین قوانین مؤثر، ایجاد نهادهای نظارتی قوی و اجرای اقدامات پیشگیرانه باشد. بررسی تطبیقی سیاست‌های جنایی اتحادیه اروپا و ایالات متحده آمریکا نشان می‌دهد که این کشورها با وجود تفاوت‌های ساختاری، بر اهمیت پیشگیری و آموزش تأکید دارند. ایران نیز باید با توجه به نقاط قوت و ضعف موجود، اقداماتی را برای بهبود وضعیت خود در این زمینه انجام دهد. در مقایسه با اتحادیه اروپا و ایالات متحده، نظام حقوقی ایران در حوزه مبارزه با بزه‌های پولی - بانکی پیشرفت‌هایی داشته، اما همچنان چالش‌هایی نظیر عدم تطبیق کامل با استانداردهای FATF، ضعف نظارتی و نبود قوانین جامع در حوزه فناوری‌های مالی وجود دارد. اجرای پیشنهادهای مطرح‌شده می‌تواند موجب افزایش شفافیت مالی، کاهش فساد اقتصادی و بهبود جایگاه ایران در نظام بانکی بین‌المللی شود.

۶- چالش‌ها و راهکارهای بهبود سیاست‌های جنایی ایران

سیاست‌های جنایی ایران در قبال بزه‌های پولی - بانکی با چالش‌های متعددی روبه‌رو است که ناشی از تحولات فناوری، پیچیدگی‌های جرایم مالی و خلأهای قانونی در مواجهه با این نوع بزهکاری‌هاست. این چالش‌ها نیازمند اصلاحات ساختاری و اجرایی در قوانین، تقویت نظارت بانکی و بهره‌گیری از فناوری‌های نوین در کشف و مقابله با این جرایم است. در این بخش ابتدا مهم‌ترین چالش‌های موجود بررسی و سپس راهکارهای پیشنهادی برای بهبود سیاست‌های جنایی ایران ارائه می‌شود.

۶-۱- چالش‌ها

مبارزه با بزه‌های پولی - بانکی در ایران با چالش‌های متعددی مواجه است که می‌تواند به‌طور مستقیم بر اثربخشی سیاست‌های جنایی تأثیر بگذارد. این چالش‌ها شامل عدم هماهنگی بین نهادهای مختلف، کمبود منابع و آموزش و ضعف در اجرای قوانین است.

۶-۱-۱- عدم هماهنگی بین نهادها

یکی از بزرگ‌ترین چالش‌ها در مبارزه با بزه‌های مالی در ایران، عدم هماهنگی و همکاری بین نهادهای مختلف نظارتی و قضایی است. نهادهایی مانند سازمان اطلاعات سپاه، پلیس فتا و سازمان امور مالیاتی هرکدام وظایف خاص خود را دارند، اما اغلب در عمل همکاری لازم را ندارند. این عدم هماهنگی می‌تواند منجر به ایجاد خلأهای قانونی و اجرایی شود که مجرمین از آن بهره‌برداری می‌کنند (FATF, 2021).

۶-۱-۲- کمبود منابع و آموزش

کمبود منابع مالی و انسانی برای نهادهای نظارتی، یکی دیگر از چالش‌های مهم است. بسیاری از نهادها با کمبود بودجه و نیروی انسانی مواجه هستند که می‌تواند بر کیفیت نظارت و اجرای قوانین تأثیر بگذارد (Transparency International, 2020). همچنین آموزش کارکنان نهادهای نظارتی درباره روش‌های جدید بزهکاری و تکنیک‌های شناسایی تخلفات مالی نیز ضروری است.

۶-۱-۳- ضعف در اجرای قوانین

علی‌رغم وجود قوانین مناسب، ضعف در اجرای مؤثر آنها یکی دیگر از چالش‌های جدی است. فساد اداری و عدم اراده سیاسی برای مقابله با بزه‌های مالی می‌تواند مانع از اجرای مؤثر قوانین شود (Transparency International, 2020).

۶-۲- اصلاحات پیشنهادی در قوانین و مقررات ایران

برای بهبود وضعیت موجود و مقابله مؤثر با بزه‌های پولی - بانکی، اصلاحات قانونی ضروری است. این اصلاحات باید شامل بازنگری در قوانین موجود و تدوین قوانین جدید باشد که بتوانند با چالش‌های کنونی سازگار شوند.

۶-۲-۱- ضرورت بازنگری در قوانین مبارزه با پول‌شویی و تأمین مالی تروریسم

یکی از چالش‌های اصلی در سیاست جنایی ایران، ناهماهنگی و خلأهای قانونی در مبارزه با پول‌شویی و سوءاستفاده از فناوری‌های مالی است. قوانین مرتبط ازجمله قانون مبارزه با

پول‌شویی مصوب ۱۳۸۶ و اصلاحیه ۱۳۹۷، هنوز در برخی زمینه‌ها ابهام دارند و نیازمند بازنگری هستند (قانون مبارزه با پول‌شویی، ۱۳۹۷). برای نمونه تعریف روشنی از نقش فناوری‌های مالی در تسهیل پول‌شویی ارائه نشده و ضمانت اجراهای کافی برای تخلفات مرتبط با فین‌تک‌ها پیش‌بینی نشده است.

۶-۲-۲- تدوین مقررات ویژه برای جرایم مالی مرتبط با فین‌تک‌ها

فناوری‌های مالی به سرعت در حال گسترش هستند و در عین تسهیل خدمات مالی، زمینه‌ساز تخلفات جدیدی همچون هک حساب‌های بانکی، کلاهبرداری دیجیتال و سوءاستفاده از ارزهای دیجیتال شده‌اند. با این حال در قانون جرایم رایانه‌ای مصوب ۱۳۸۸، صراحتی درباره نحوه برخورد با جرایم مرتبط با فین‌تک‌ها وجود ندارد (قانون جرایم رایانه‌ای، ۱۳۸۸). از این رو پیشنهاد می‌شود تا مقرراتی خاص برای تنظیم فعالیت‌های فین‌تک‌ها همراه با نظارت بر تراکنش‌های مالی آنها تدوین شود.

۶-۲-۳- هماهنگ‌سازی قوانین ایران با استانداردهای بین‌المللی

یکی دیگر از نواقص سیاست جنایی ایران، عدم تطابق کامل با استانداردهای گروه ویژه اقدام مالی (FATF) است. ایران هنوز در فهرست کشورهای قرار دارد که نیاز به اصلاحات در قوانین مبارزه با پول‌شویی و تأمین مالی تروریسم دارند (FATF, 2022). لازم است ایران با اصلاح قوانین، الزامات بین‌المللی را رعایت کند تا هم از تحریم‌های مالی جلوگیری شود و هم امکان همکاری بین‌المللی در مقابله با جرایم مالی فراهم گردد.

۶-۲-۴- ایجاد نظام یکپارچه اطلاعاتی

ایجاد یک نظام یکپارچه اطلاعاتی برای شناسایی و پیگیری فعالیت‌های مشکوک می‌تواند به بهبود وضعیت کمک کند. این سیستم باید اطلاعات مربوط به تراکنش‌های مالی را از تمامی مؤسسات مالی جمع‌آوری کند و امکان تحلیل داده‌ها را فراهم آورد (FATF, 2021).

۶-۲-۵- تقویت قوانین مربوط به شفافیت مالی

تدوین قوانین جدید برای افزایش شفافیت مالی در بخش خصوصی و دولتی می‌تواند به کاهش تخلفات مالی کمک کند. این قوانین باید شامل الزام به افشای اطلاعات مالی برای شرکت‌ها و مؤسسات باشد تا نظارت بر فعالیت‌های مالی آسان‌تر شود (گزارش جهانی فساد، ۲۰۲۰).

۶-۳- راهکارهای تقویت نظارت بانکی و پیشگیری از تخلفات مالی

تقویت نظارت بانکی و پیشگیری از تخلفات مالی نیازمند اتخاذ راهکارهای جامع و مؤثر است که بتواند به بهبود وضعیت کمک کند.

۶-۳-۱- ایجاد سامانه‌های هوشمند نظارتی

یکی از مهم‌ترین اقدامات در مبارزه با جرایم پولی - بانکی، راه‌اندازی سامانه‌های تحلیل داده و نظارت بر تراکنش‌های مالی مشکوک است. در کشورهای پیشرفته از الگوریتم‌های هوش مصنوعی برای رصد و تحلیل رفتارهای غیرعادی مالی استفاده می‌شود (World Bank, 2021). در ایران بانک مرکزی باید با توسعه سامانه‌هایی مشابه، امکان شناسایی سریع‌تر جرایم مالی را فراهم کند.

۶-۳-۲- تقویت نقش بانک‌ها در گزارش‌دهی تخلفات

بر اساس قانون، بانک‌ها موظف به گزارش تراکنش‌های مشکوک به واحد اطلاعات مالی هستند، اما در عمل بسیاری از تخلفات به دلیل عدم همکاری کامل بانک‌ها و نبود رویه‌های مشخص، گزارش نمی‌شوند (مرکز پژوهش‌های مجلس، ۱۴۰۰). برای حل این مشکل باید بانک‌ها مکلف شوند که در دوره‌های مشخص، گزارش‌هایی در مورد تراکنش‌های مشکوک ارائه داده و در صورت تخلف با ضمانت اجراهای جدی مواجه شوند.

۶-۳-۳- نظارت بر فعالیت‌های مالی در بستر رمزارزها

یکی از چالش‌های جدید در نظام بانکی استفاده از رمزارزها برای پول‌شویی و فرار مالیاتی است. در حال حاضر قوانین روشنی برای نظارت بر معاملات رمزارزی در ایران وجود ندارد و این مسئله فضای مناسبی برای سوءاستفاده ایجاد کرده است (International Monetary Fund (IMF), 2022). پیشنهاد می‌شود که بانک مرکزی یک چهارچوب قانونی شفاف برای نظارت بر صرافی‌های رمزارزی و کنترل تراکنش‌های دیجیتال تدوین کند.

۶-۳-۴- افزایش آگاهی عمومی

افزایش آگاهی عمومی درباره خطرات بزه‌های مالی و روش‌های پیشگیری می‌تواند به کاهش وقوع این جرایم کمک کند. برنامه‌های آموزشی برای عموم مردم و کارکنان مؤسسات مالی ضروری است تا بتوانند بهتر از خود محافظت کنند (گزارش جهانی فساد، ۲۰۲۰).

۶-۴- استفاده از فناوری‌های نوین در کشف و مقابله با بزه‌های پولی - بانکی

فناوری‌های نوین می‌توانند نقش مهمی در کشف و مقابله با بزه‌های پولی - بانکی ایفا کنند.

۶-۴-۱- بهره‌گیری از هوش مصنوعی در تحلیل جرایم مالی

هوش مصنوعی و یادگیری ماشینی^{۲۹} می‌توانند در کشف تخلفات مالی نقش مؤثری ایفا کنند.

کشورهای پیشرفته از مدل‌های پردازش کلان‌داده برای تحلیل رفتارهای مالی مشکوک استفاده می‌کنند (OECD, 2021). ایران نیز می‌تواند با استفاده از فناوری‌های مشابه، فرایند شناسایی و پیگیری جرایم مالی را بهبود ببخشد.

۶-۴-۲- توسعه بانک‌های اطلاعاتی یکپارچه

در حال حاضر اطلاعات مالی در ایران به‌صورت پراکنده در نهادهای مختلف نظیر بانک مرکزی، سازمان امور مالیاتی و پلیس فتا نگهداری می‌شود. عدم یکپارچگی این داده‌ها، روند کشف تخلفات را دشوار کرده است (مرکز پژوهش‌های مجلس، ۱۴۰۰). پیشنهاد می‌شود یک سامانه جامع ملی برای تجمیع و تحلیل اطلاعات مالی مشکوک راه‌اندازی شود تا همکاری میان نهادهای نظارتی افزایش یابد.

۶-۴-۳- استفاده از بلاکچین برای افزایش شفافیت مالی

فناوری بلاکچین^{۳۰} یکی از ابزارهای مؤثر در افزایش شفافیت مالی و جلوگیری از جرایم پول‌شویی است. برخی کشورها از این فناوری برای ثبت غیرقابل تغییر تراکنش‌های مالی و احراز هویت دیجیتال استفاده می‌کنند (European Central Bank, 2022). ایران نیز می‌تواند از بلاکچین در سیستم‌های بانکی برای کاهش تقلب و افزایش امنیت مالی بهره بگیرد. فناوری بلاکچین امکان ثبت دائمی تراکنش‌ها را فراهم می‌آورد که می‌تواند مانع از تغییر یا حذف اطلاعات شود (Catalini & Gans, 2016).

۶-۴-۴- سیستم‌های نظارتی مبتنی بر داده

استفاده از سیستم‌های نظارتی مبتنی بر داده می‌تواند به نهادهای نظارتی کمک کند تا به‌طور مؤثرتری بر روی فعالیت‌های مالی نظارت کنند. این سیستم‌ها باید قادر به جمع‌آوری و تحلیل داده‌ها از منابع مختلف باشند تا بتوانند الگوهای مشکوک را شناسایی کنند (Gonzalez et al., 2018).

مبارزه با بزه‌های پولی - بانکی نیازمند یک رویکرد جامع است که شامل اصلاحات قانونی، تقویت نظارت بانکی و استفاده از فناوری‌های نوین باشد. با توجه به چالش‌های موجود، ایران باید اقداماتی را برای بهبود وضعیت خود انجام دهد تا بتواند با بزهکاری مالی به‌طور مؤثر مقابله کند. سیاست‌های جنایی ایران در مواجهه با بزه‌های پولی - بانکی نیازمند اصلاحات بنیادین در سطح تقنینی، اجرایی و نظارتی است. از مهم‌ترین چالش‌ها می‌توان به خلأهای قانونی، نبود هماهنگی با استانداردهای بین‌المللی و ضعف در نظارت بانکی اشاره کرد. برای بهبود وضعیت پیشنهاد می‌شود که قوانین مبارزه با پول‌شویی و جرایم مالی به‌روزرسانی شوند، بانک‌ها نقش فعال‌تری در

گزارش‌دهی تخلفات ایفا کنند و فناوری‌های نوین مانند هوش مصنوعی، بلاکچین و سامانه‌های تحلیلی برای مقابله با این جرایم به کار گرفته شوند. این اصلاحات می‌توانند منجر به افزایش شفافیت، کاهش جرایم پولی - بانکی و بهبود همکاری‌های بین‌المللی در حوزه مالی شوند.

نتیجه‌گیری و پیشنهادها

سیاست‌های جنایی ایران در قبال بزه‌های پولی - بانکی با چالش‌های متعددی مواجه است که ناشی از تحولات فناوری، پیچیدگی‌های جرایم مالی و ضعف نظارتی است. با توجه به افزایش موارد پول‌شویی، کلاهبرداری دیجیتال و سوءاستفاده از فناوری‌های مالی، سیاست‌های جنایی کشور نیازمند اصلاحات عمیق در ابعاد تقنینی، قضایی و اجرایی است. این پژوهش با بررسی قوانین داخلی، رویه‌های قضایی، سیاست‌های اجرایی و مقایسه تطبیقی با اتحادیه اروپا و ایالات متحده آمریکا، به تحلیل نقاط ضعف و قوت سیاست‌های جنایی ایران پرداخته و پیشنهادهایی برای بهبود آن ارائه کرده است. بررسی‌های انجام‌شده نشان می‌دهد که سیاست جنایی ایران در برابر جرایم پولی - بانکی ترکیبی از اقدامات تقنینی، قضایی و اجرایی است، اما این سیاست‌ها دارای کاستی‌های عمده‌ای هستند:

۱. در حوزه تقنینی:

- قوانین مرتبط با پول‌شویی و سوءاستفاده از فناوری‌های مالی همچنان دارای خلأهای حقوقی هستند (قانون مبارزه با پول‌شویی، ۱۳۹۷).
- تعریف دقیقی از برخی روش‌های جدید ارتکاب جرم از طریق فناوری‌های مالی ارائه نشده است (قانون جرایم رایانه‌ای، ۱۳۸۸).
- قوانین مرتبط با نظارت بر فعالیت‌های فین‌تک‌ها و رمزارزها نامشخص است (International Monetary Fund (IMF), 2022).

۲. در حوزه قضایی:

- رویه‌های قضایی در برخورد با جرایم مالی همچنان دارای تناقض و ناهماهنگی است.
- دادگاه‌ها به دلیل عدم آشنایی کافی با فناوری‌های مالی، در برخی موارد با مشکلات تفسیری مواجه هستند.

۳. در حوزه اجرایی:

- نظارت بر فعالیت بانک‌ها، مؤسسات مالی و صرافی‌های دیجیتال ضعیف است (مرکز پژوهش‌های مجلس، ۱۴۰۰).
- سامانه‌های تحلیل و کشف تخلفات مالی مبتنی بر داده‌های کلان و هوش مصنوعی در کشور توسعه نیافته است (World Bank, 2021).

مطالعات تطبیقی نشان می‌دهد که اتحادیه اروپا و ایالات متحده آمریکا رویکردهای جامعی در مبارزه با جرایم پولی - بانکی اتخاذ کرده‌اند. در اتحادیه اروپا، قوانین مرتبط با شفافیت مالی، تراکنش‌های مشکوک و مجازات‌های سنگین برای بانک‌ها و شرکت‌های فین‌تک تصویب شده است (European Central Bank, 2022). در ایالات متحده آمریکا نیز نهادهای نظارتی همچون SEC و FBI نقش فعالی در رصد تخلفات مالی و مبارزه با پول‌شویی دارند (FATF, 2022). ایران برای رسیدن به استانداردهای بین‌المللی نیاز به اصلاحات گسترده‌ای در حوزه تقنین، اجرا و نظارت بانکی دارد.

پیشنهادهای اجرایی برای بهبود سیاست‌های جنایی ایران

- بازنگری در قانون مبارزه با پول‌شویی و اضافه کردن مقررات مشخص درباره فین‌تک‌ها و تراکنش‌های دیجیتال.
- تدوین قانون ویژه برای رمزارزها که شامل نظارت بر صرافی‌های رمزارزی، نحوه احراز هویت کاربران و ردیابی تراکنش‌ها باشد.
- ایجاد ضمانت اجرای شدیدتر برای بانک‌ها و مؤسسات مالی که در گزارش‌دهی تراکنش‌های مشکوک کوتاهی می‌کنند.

اصلاحات اجرایی

- ایجاد سامانه‌های هوشمند تحلیل داده‌های بانکی برای کشف جرایم مالی و تراکنش‌های مشکوک.
- الزام بانک‌ها و شرکت‌های فین‌تک به به‌کارگیری فناوری‌های احراز هویت بیومتریک و احراز هویت مشتری.
- تشدید نظارت بر صرافی‌های رمزارزی و ایجاد دستورالعمل‌های نظارتی مشخص برای آنها.

اصلاحات قضایی

- برگزاری دوره‌های تخصصی آموزشی برای قضات و دادستان‌ها در زمینه جرایم مالی، رمزارزها و فناوری‌های مالی.
- ایجاد دادگاه‌های ویژه جرایم مالی برای بررسی سریع‌تر و تخصصی‌تر پرونده‌های مرتبط.
- تسهیل همکاری بین نهادهای نظارتی داخلی و پلیس بین‌الملل^{۳۱} در پرونده‌های مربوط به پول‌شویی و کلاهبرداری بین‌المللی.

ایران هنوز در فهرست خاکستری FATF قرار دارد و برای خروج از آن، باید قوانین مبارزه با پولشویی و تأمین مالی تروریسم را اصلاح کند. این اصلاحات می‌تواند شامل افزایش شفافیت بانکی، ایجاد سامانه‌های ثبت تراکنش‌های مشکوک و تشدید نظارت بر بانک‌ها باشد. بسیاری از تخلفات پولی - بانکی به شبکه‌های بین‌المللی جرایم سازمان‌یافته مرتبط است. برای مقابله با این جرایم، ایران باید:

- همکاری خود را با نهادهای بین‌المللی مانند اینترپل و بانک جهانی افزایش دهد.
- به معاهدات بین‌المللی مبارزه با جرایم مالی و پولشویی بپیوندد.
- مکانیسم‌هایی برای ردیابی بین‌المللی تراکنش‌های مشکوک ایجاد کند.

کشورهای توسعه‌یافته سیستم‌های نظارتی و مجازات‌های شدیدی برای تخلفات مالی وضع کرده‌اند که ایران نیز می‌تواند از آنها الگوبرداری کند. به‌طور مثال در آمریکا، قانون رازداری بانکی (BSA)، بانک‌ها را ملزم به گزارش تراکنش‌های مشکوک می‌کند و در اتحادیه اروپا، دستورالعمل پنجم مبارزه با پولشویی^{۳۲}، فین‌تک‌ها را تحت نظارت مالی قرار می‌دهد. ایران نیز می‌تواند با اجرای سیستم‌های مشابه، شفافیت مالی و سطح مبارزه با جرایم پولی - بانکی را افزایش دهد. این پژوهش نشان داد که سیاست‌های جنایی ایران در قبال بزه‌های پولی - بانکی دارای نواقصی در سطح تقنین، اجرا و نظارت است. در مقایسه با اتحادیه اروپا و ایالات متحده آمریکا، سیاست‌های ایران نیازمند اصلاحاتی همچون بازنگری در قوانین، توسعه سامانه‌های نظارتی و تشدید ضمانت اجرای بانکی است. پیشنهاد می‌شود که ایران سیاست‌های جنایی خود را با استانداردهای بین‌المللی هماهنگ کند و از فناوری‌های نوین مانند بلاکچین و هوش مصنوعی برای کشف و پیشگیری از تخلفات مالی بهره گیرد.

منابع فارسی

الف) منابع فارسی

- دادستانی کل کشور. (۱۳۹۷). گزارش عملکرد دادستانی کل کشور درباره پرونده فساد سه هزار میلیاردی. تهران.
- عزیزی، آریا. (۱۳۹۷). نقش بانک‌ها و مؤسسات اعتباری در رونق اقتصاد ملی. فصلنامه مطالعات نوین بانکی، ۱(۱).
- قاسمی، ناصر. (۱۴۰۰). فرصت‌ها و تهدیدات ارزهای دیجیتال؛ مطالعه موردی شرق منتخب کشورهای آسیایی. فصلنامه جهان سیاست، ۱۰(۳).
- قانون بانکداری بدون ربا، مصوب ۱۳۶۲.
- قانون جرایم رایانه‌ای، مصوب ۱۳۸۸.
- قانون مبارزه با پول‌شویی، مصوب ۱۳۸۶، اصلاحیه ۱۳۹۷.
- قانون مبارزه با تأمین مالی تروریسم، مصوب ۱۳۹۴.
- گزارش سالانه بانک مرکزی جمهوری اسلامی ایران. (۱۴۰۰).
- گزارش سالانه سازمان بورس و اوراق بهادار. (۱۴۰۰).
- گزارش عملکرد پلیس فتا. (۱۴۰۱).
- گسن، رمون. (۱۳۹۳). جرم‌شناسی بزهکاری اقتصادی: نظریه مومی تزویری. ترجمه شهرام ابراهیمی. تهران: نشر میزان.
- مرکز پژوهش‌های مجلس شورای اسلامی. (۱۴۰۰). تحلیل سیاست‌های جنایی ایران در حوزه جرایم مالی. تهران: مرکز پژوهش‌های مجلس.
- مرکز پژوهش‌های مجلس شورای اسلامی. (۱۴۰۰). گزارش وضعیت جرایم پولی - بانکی در ایران. تهران: مرکز پژوهش‌های مجلس.
- میرزایی منفرد، غلامعلی. (۱۳۸۹). حقوق کیفری اوراق بهادار. تهران: نشر میزان.
- میرسعیدی، سید منصور و محمود زمانی. (۱۳۹۲). جرم اقتصادی، تعریف یا ضابطه؟. فصلنامه پژوهش حقوق کیفری، ۲.
- میرمحمدصادقی، حسین. (۱۳۹۲). جرایم علیه امنیت و آسایش عمومی. چاپ بیست و سوم. تهران: نشر میزان.
- نورزاد، مجتبی. (۱۳۸۹). جرایم اقتصادی در حقوق کیفری ایران. تهران: نشر جنگل، جاودانه.

ب) منابع انگلیسی

- Aldawood, H., & G. Skinner. (2019). Reviewing cyber security social engineering training and awareness programs - Pitfalls and opportunities. *Computers & Security*, 87.
- Arner, D. W., J. Barberis & R. P. Buckley. (2016). The evolution of FinTech: A new post-crisis paradigm?. *Georgetown Journal of International Law*, 47(4).
- Carlisle, D. (2021). Cryptocurrencies and terrorist financing: A risk, but not a revolution. *RUSI Journal*, 166(4).

- Catalini, C., & J. S. Gans. (2016). *Some Simple Economics of the Blockchain*. National Bureau of Economic Research.
- European Central Bank. (2022). Anti-Money Laundering and Financial Crimes.
- European Central Bank. (2022). Blockchain and Financial Transparency.
- European Commission. (2020). Anti-Money Laundering Directive.
- European Union Agency for Law Enforcement Cooperation. (2021). Annual Report.
- FATF. (2021). Money laundering and the misuse of cryptocurrencies. Paris: Financial Action Task Force.
- FATF. (2021). Mutual Evaluation Report.
- FATF. (2022). Financial Action Task Force Annual Report.
- FATF. (2022). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. Paris: Financial Action Task Force.
- Gandal, N., J. T. Hamrick, T. Moore, & T. Oberman. (2018). Price Manipulation in the Bitcoin Ecosystem. *Journal of Monetary Economics*, 95.
- Gonzalez, R., et al. (2018). Data-driven Approaches to Financial Crime Prevention. *Journal of Financial Crime*.
- Gottschalk, P. (2018). *White-collar crime and fraud investigation*. Routledge.
- International Monetary Fund (IMF). (2022). Crypto Assets and Anti-Money Laundering Policies.
- Kumar, N., S. Marchal, A. Francillon & T. Engel. (2019). Cryptojacking: A primer on illicit cryptocurrency mining. *Journal of Cyber Security*, 5(3).
- Levi, M. (2010). Combating financial crime: The role of financial services regulation. *Journal of Financial Crime*, 17(3). 236-252.
- Momtaz, P. P. (2020). Initial coin offerings: Financing growth with cryptocurrency token sales. *Journal of Corporate Finance*, 65.
- Marr, B. (2019). *Artificial intelligence in practice: How 50 successful companies used AI and machine learning to solve problems*. Wiley.
- Martin, J. (2014). Lost on the Silk Road: Online Drug Distribution and the Cryptomarket. *Criminology & Criminal Justice*, 14(3).
- OECD. (2021). AI in Financial Crime Prevention.
- OECD. (2022). *Digital finance and financial crime: Emerging risks and regulatory challenges*. Paris: OECD Publishing.
- Rose-Ackerman, S., & B. J. Palifka. (2016). *Corruption and government: Causes, consequences, and reform*. Cambridge: Cambridge University Press.
- Savona, E. U. & M. Riccardi (Eds.). (2017). *Corruption, Economic Crime and Globalization*. Routledge.
- Transparency International. (2020). *Corruption Perceptions Index 2020*. Berlin: Transparency International.
- U.S. Department of Justice. (2020). Annual Report on Financial Crime.
- U.S. Department of the Treasury. (2021). Bank Secrecy Act.
- United Nations. (2003). United Nations Convention against Corruption.
- Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.
- World Bank. (2021). Digital Finance and Financial Crimes.
- World Bank. (2021). Financial Crime and Digital Technologies.
- Zabyelina, Y., & D. Van Uhm (Eds.). (2020). *Illegal Mining: Organized Crime*,

Corruption, and Ecocide in a Resource-Scarce World. Cham: Palgrave Macmillan.

- Zarate, J. (2019). *Treasury's war: The unleashing of a new era of financial warfare*. PublicAffairs.

- Zetsche, D. A., R. P. Buckley, J. N. Barberis & D. W. Arner. (2017). Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation. *Fordham Journal of Corporate & Financial Law*, 23(1).

- Zhang, Y., et al. (2020). Artificial Intelligence in Financial Services: A Review. *Journal of Financial Services Research*.